Panduan Pengguna

AWS Hub Keamanan



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Hub Keamanan: Panduan Pengguna

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau mungkin tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu Security Hub dan Security Hub CSPM? 1
AWS Hub Keamanan 2
Fitur 2
Integrasi 3
Mengakses Hub Keamanan 4
Konsep 4
Penaksir Biaya 10
Akses berdasarkan jenis akun 11
Prasyarat 12
Menyiapkan akses lintas akun 13
Menggunakan penaksir biaya 16
Catatan penting 23
Informasi Terkait 24
Mengaktifkan Hub Keamanan 24
Aktifkan Hub Keamanan untuk AWS Organisasi 25
Aktifkan Hub Keamanan di akun mandiri 27
Menunjuk administrator yang didelegasikan 28
Membuat kebijakan administrator yang didelegasikan 30
Mengelola konfigurasi akun anggota 31
Menghapus administrator yang didelegasikan 36
Re-enabling Hub Keamanan 37
Rekomendasi 38
Cakupan akun 39
Halaman cakupan akun 40
Widget cakupan keamanan 42
Paket diperpanjang 42
Izin untuk Paket Diperpanjang 42
Mendaftar untuk mitra paket Extended 43
Berhenti berlangganan dari mitra 43
Cross-Region agregasi 44
Jenis data yang digabungkan 44
Agregasi untuk akun administrator dan anggota 46
Aturan otomatisasi dan agregasi lintas wilayah 46
Mengaktifkan agregasi 47

Meninjau pengaturan agregasi 48
Memperbarui pengaturan agregasi 48
Menghapus agregasi 49
Integrasi dengan Azure 50
Bagaimana AWS Config digunakan 52
Informasi tambahan 52
Prasyarat 53
Mengkonfigurasi Azure 55
Mengonfigurasi Security Hub 66
Menghapus konektor Azure 78
Dasbor ringkasan 79
Pertimbangan-pertimbangan 79
Widget yang tersedia 80
Filter yang tersedia 93
Melihat detail tentang sumber daya di Hub Keamanan 94
Menemukan format: OCSF 96
Ikhtisar OCSF 96
Sumber daya terkait 96
AWS ekstensi untuk OCSF 96
Temuan cakupan 119
Temuan cakupan untuk AWS Hub Keamanan CSPM 119
Temuan cakupan untuk Amazon GuardDuty 120
Temuan cakupan untuk Amazon Inspector 120
Temuan cakupan untuk Amazon Macie 121
Menekan temuan cakupan 121
Inventaris AI 122
Prasyarat untuk penemuan AI yang dihosting sendiri 122
Jenis sumber daya AI yang didukung 123
Menemukan sumber daya AI dari halaman Sumber Daya 123
Menggunakan halaman inventaris AI 124
Pertimbangan-pertimbangan 125
Mengakses inventaris AI dengan API 126
Temuan eksposur 127
Bagaimana temuan eksposur bekerja 128
Komponen temuan eksposur 129
Klasifikasi tingkat keparahan 131

Manfaat temuan eksposur 131
Sumber temuan paparan 131
Praktik terbaik 132
Sumber daya yang didukung 133
Sifat yang didukung 134
Menghasilkan temuan eksposur 136
Menentukan tingkat keparahan temuan eksposur 141
Meninjau temuan eksposur 143
Grafik jalur serangan potensial 145
Memperbaiki temuan paparan 146
Temuan akses yang tidak digunakan 250
Cara kerja analisis akses yang tidak digunakan 250
Jenis pencarian akses yang tidak digunakan 251
Service-linked penganalisis 251
Melihat temuan akses yang tidak digunakan 252
Akses yang tidak digunakan dalam temuan eksposur 252
Rekomendasi kebijakan untuk izin yang tidak digunakan 253
Harga 253
Rekomendasi kebijakan 253
Bagaimana rekomendasi kebijakan bekerja 253
Siapa yang bisa menghasilkan rekomendasi 254
Siklus hidup rekomendasi 254
Kasus kesalahan 254
Menggunakan konsol 255
Referensi API 255
Pemindaian Jaringan 255
Jenis sumber daya yang didukung 256
Aktifkan Pemindaian Jaringan 256
Cara kerja Pemindaian Jaringan 258
Temuan Pemindaian Jaringan 258
Pindai bukti 261
Mengecualikan sumber daya dari pemindaian 262
Port yang didukung 262
Multi-cloud dukungan 262
Ketersediaan wilayah 263
Nonaktifkan Pemindaian Jaringan 263

Otomatisasi 264
Aturan otomatisasi 265
EventBridge aturan otomatisasi 283
Third-party integrasi 3
Jira Cloud 292
ServiceNow 298
Kebijakan utama KMS untuk integrasi tiket 305
Menguji integrasi tiket 308
Aplikasi MCP (Pratinjau) 311
Contoh Aplikasi MCP 311
Konsep Utama 315
Prasyarat 316
Menyiapkan server MCP 316
Menggunakan Diagnostik Konektor 317
Alat yang tersedia 318
Memantau penggunaan dan biaya 319
Siapa yang dapat mengakses halaman Penggunaan 319
Ringkasan biaya organisasi dan akun 320
Tampilan Kemampuan 321
Tampilan Akun 322
Strategi optimasi biaya 323
Sumber daya terkait 323
Menonaktifkan Hub Keamanan 323
Menonaktifkan Hub Keamanan untuk satu akun 323
Menonaktifkan Hub Keamanan di seluruh organisasi 324
Keamanan 326
Perlindungan data 327
Manajemen identitas dan akses 330
Validasi kepatuhan 363
Ketahanan 364
Keamanan infrastruktur 364
Titik akhir VPC (AWS PrivateLink) 365
Mencatat panggilan API 366
Informasi Security Hub di CloudTrail 367
Contoh: Entri file log Hub Keamanan 368
AWS Hub Keamanan CSPM 371

Manfaat Security Hub CSPM 372
Mengakses Hub Keamanan CSPM 373
Layanan terkait 375
Security Hub CSPM uji coba gratis, penggunaan, dan harga 375
Melihat detail penggunaan 375
Detail harga 376
Konsep 376
Mengaktifkan Security Hub CSPM 382
Memverifikasi izin yang diperlukan 382
Mengaktifkan Security Hub CSPM dengan integrasi Organisasi 382
Mengaktifkan Security Hub CSPM secara manual 385
Langkah selanjutnya: Manajemen postur dan integrasi 387
Mengkonfigurasi AWS Config 387
Konfigurasi lokal 394
Konfigurasi pusat 395
Mengelola beberapa akun 443
Mengelola akun denganAWS Organizations 443
Mengelola akun secara manual dengan undangan 444
Rekomendasi untuk lingkungan multi-akun 445
Mengelola akun dengan AWS Organizations 447
Mengelola akun dengan undangan 463
Tindakan yang diizinkan oleh administrator dan akun anggota 477
Pengaruh tindakan akun pada data 483
Menggabungkan data di seluruh Wilayah 486
Jenis data yang dikumpulkan 487
Agregasi untuk akun administrator dan anggota 489
Konfigurasi dan agregasi pusat 490
Mengaktifkan agregasi 491
Meninjau pengaturan agregasi 493
Memperbarui pengaturan agregasi 494
Menghentikan agregasi 496
Standar 497
Referensi standar 499
Mengaktifkan standar 589
Meninjau detail standar 596
Mematikan standar yang diaktifkan secara otomatis 599

Menonaktifkan standar 600
Kontrol 603
Tampilan kontrol terkonsolidasi 604
Ringkasan skor keamanan untuk kontrol 605
Referensi kontrol 606
Izin untuk mengonfigurasi kontrol 1495
Mengaktifkan kontrol 1496
Menonaktifkan kontrol 1505
Pemeriksaan dan skor keamanan 1515
Kategori kontrol 1591
Meninjau detail kontrol 1594
Kontrol penyaringan dan penyortiran 1597
Parameter kontrol 1598
Meninjau dan mengelola temuan kontrol 1612
Integrasi 1641
Meninjau daftar integrasi 1642
Mengaktifkan aliran temuan dari integrasi 1643
Menonaktifkan aliran temuan dari integrasi 1644
Melihat temuan dari integrasi 1645
Layanan AWS integrasi 1646
Third-party integrasi 1668
Integrasi produk kustom 1703
Integrasi dengan Azure 1706
Bagaimana AWS Config digunakan 1707
Jenis konektor 1707
Prasyarat 1708
Mengkonfigurasi Azure 1711
Mengkonfigurasi Security Hub CSPM 1717
Menghapus konektor Azure 1738
Temuan 1739
BatchImportFindings untuk menemukan penyedia 1741
BatchUpdateFindings untuk pelanggan 1744
Meninjau detail dan sejarah temuan 1748
Memfilter temuan 1753
Mengelompokkan temuan 1755
Mengatur status alur kerja temuan 1756

Mengirim temuan ke tindakan khusus 1759
Format pencarian: ASFF 1760
Wawasan 2054
Meninjau dan bertindak berdasarkan wawasan 2055
Wawasan terkelola 2057
Wawasan khusus 2068
Otomatisasi 2075
Aturan otomatisasi 2076
Respon dan remediasi otomatis 2103
Dasbor ringkasan 2119
Widget yang tersedia untuk dasbor Ringkasan 2120
Memfilter dasbor 2124
Menyesuaikan dasbor 2126
Batas regional 2126
Cross-Region pembatasan agregasi 2127
Ketersediaan integrasi menurut Wilayah 2127
Ketersediaan standar menurut Wilayah 2129
Ketersediaan kontrol berdasarkan Wilayah 2130
Batasan regional pada kontrol 2130
Menciptakan sumber daya dengan CloudFormation 2386
Security Hub CSPM danCloudFormationtemplat 2387
Pelajari lebih lanjut tentangCloudFormation 2387
Berlangganan pengumuman 2388
Format pesan Amazon SNS 2393
Menonaktifkan CSPM Security Hub 2395
Keamanan 2398
Perlindungan data 2399
Manajemen identitas dan akses 2400
Validasi kepatuhan 2435
Ketahanan 2436
Keamanan infrastruktur 2436
Titik akhir VPC (AWS PrivateLink) 2437
Mencatat panggilan API 2438
Informasi CSPM Security Hub di CloudTrail 367
Contoh: Entri file log CSPM Security Hub 368
Memberikan tag ke sumber daya 2442

Menandai dasar-dasar 2442
Menggunakan tag dalam kebijakan IAM 2444
Menambahkan tag ke sumber daya 2445
Mengedit tag untuk sumber daya 2448
Meninjau tag untuk sumber daya 2450
Menghapus tag dari sumber daya 2452
Kuota 2455
Kuota maksimum 2455
Nilai kuota 2455
Riwayat dokumen 2456
..... mmdlxix

Apa itu Security Hub dan Security Hub CSPM?

AWSSecurity Hub dan AWS Security Hub CSPM adalah Layanan AWS yang melindungi lingkungan cloud Anda. Layanan saling melengkapi. Ketika digunakan bersama, mereka memberikan wawasan berharga tentang postur keamanan AWS lingkungan Anda.

Security Hub CSPM memberikan pandangan komprehensif tentang postur keamanan Anda dan membantu Anda mengevaluasi lingkungan cloud Anda terhadap standar industri keamanan dan praktik terbaik. Security Hub memberikan pengalaman terpadu yang membantu Anda memprioritaskan dan menanggapi masalah keamanan kritis. Temuan CSPM Security Hub diarahkan ke Security Hub secara otomatis, di mana mereka berkorelasi dengan temuan dari layanan keamanan lain, seperti Amazon Inspector, untuk menghasilkan eksposur. Ini membantu Anda mengidentifikasi risiko paling kritis di lingkungan Anda. Security Hub juga menyediakan kemampuan alur kerja otomatis, yang membantu Anda menggabungkan temuan CSPM Security Hub ke dalam alur kerja operasional Anda.

Sebagai praktik terbaik, kami sarankan untuk mengaktifkan kedua layanan. Anda dapat mengaktifkan Security Hub CSPM tanpa mengaktifkan Security Hub jika fokus utama Anda adalah mengidentifikasi kesalahan konfigurasi dan mengevaluasi postur keamanan Anda. Namun, jika Anda mengaktifkan Security Hub tanpa mengaktifkan Security Hub CSPM, Security Hub tidak dapat menggunakan temuan CSPM Security Hub untuk memberikan informasi tentang risiko dan eksposur di lingkungan Anda. AWS Untuk pengalaman yang optimal, kami merekomendasikan tidak hanya mengaktifkan Security Hub dan Security Hub CSPM, tetapi juga mengaktifkan layanan keamanan lainnya: Amazon, Amazon GuardDuty Inspector, dan Amazon Macie.

Pengantar AWS Hub Keamanan

AWS Security Hub adalah solusi keamanan cloud terpadu yang memprioritaskan masalah keamanan kritis Anda dan membantu Anda merespons dalam skala besar. Security Hub mendeteksi masalah keamanan dengan menghubungkan dan memperkaya sinyal keamanan secara otomatis dari berbagai sumber. Sumber-sumber ini termasuk manajemen postur, manajemen kerentanan (Amazon Inspector), data sensitif (Amazon Macie), dan deteksi ancaman (Amazon GuardDuty). Gunakan Security Hub untuk memprioritaskan risiko aktif di lingkungan cloud Anda melalui analisis otomatis dan wawasan kontekstual. Melalui visualisasi intuitif, Security Hub mengubah sinyal keamanan yang kompleks menjadi wawasan yang dapat ditindaklanjuti, yang memungkinkan Anda membuat keputusan berdasarkan informasi tentang keamanan Anda dengan cepat. Security Hub juga menyertakan alur kerja respons otomatis untuk membantu Anda mengatasi risiko, meningkatkan produktivitas tim, dan meminimalkan gangguan operasional.

Fitur

Solusi keamanan terpadu

Dapatkan visibilitas yang lebih luas di seluruh lingkungan cloud Anda melalui manajemen terpusat dalam solusi keamanan cloud terpadu.

Wawasan keamanan yang dapat ditindaklanjuti

Dapatkan wawasan keamanan yang dapat ditindaklanjuti melalui analisis lanjutan untuk mempelajari risiko keamanan yang terkait dengan lingkungan Anda.

Mengurangi waktu respons

Sederhanakan waktu respons dengan alur kerja otomatis dan sistem tiket terintegrasi.

Temuan eksposur

Security Hub menghubungkan temuan dari pemeriksaan kontrol CSPM Security Hub, Amazon Inspector, dan lainnya Layanan AWS untuk mendeteksi eksposur yang terkait dengan sumber daya. AWS

Analisis akses yang tidak digunakan

Security Hub secara otomatis mengidentifikasi peran IAM, pengguna, kunci akses, dan izin yang belum digunakan dalam periode lookback 90 hari. Saat Anda mengaktifkan Hub Keamanan, layanan

akan membuat Penganalisis Akses IAM yang ditautkan ke layanan di akun Anda. Temuan akses yang tidak digunakan membantu Anda menerapkan akses hak istimewa terkecil dengan menyoroti prinsip-prinsip IAM yang disediakan secara berlebihan. Untuk temuan izin yang tidak terpakai, Security Hub dapat menghasilkan rekomendasi kebijakan hak istimewa terkecil yang menunjukkan kebijakan penggantian dengan cakupan.

Temuan diformat dalam Open Cybersecurity Schema Framework (OCSF)

Security Hub menghasilkan temuan di OCSF dan menerima temuan di OCSF dari Security Hub CSPM dan lainnya: Layanan AWS

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector

Dasbor

Konsol Security Hub menyediakan tampilan komprehensif tentang eksposur, ancaman, cakupan keamanan, dan sumber daya Anda, serta visualisasi interaktif yang disebut grafik jalur serangan, yang menunjukkan bagaimana penyerang potensial dapat mengakses dan mengendalikan sumber daya yang terkait dengan temuan eksposur.

Integrasi dengan produk pihak ketiga

Anda dapat meningkatkan postur keamanan Anda dengan integrasi Hub Keamanan. Misalnya, jika Anda menggunakan Jira Cloud atauServiceNow ITSM, Anda dapat menggunakan fitur ini untuk membuat tiket dari temuan.

Integrasi

Security Hub menerima temuan dari berikut ini Layanan AWS.

- AWS Hub Keamanan CSPM
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- Penganalisis Akses IAM

Mengakses Hub Keamanan

Security Hub tersedia di sebagian besar Wil AWS ayah. Untuk daftar Wilayah di mana Hub Keamanan saat ini tersedia, lihat titik akhir dan kuota Hub Keamanan di Referensi Umum AWS. Untuk informasi tentang mengelola Wilayah AWS untuk Anda Akun AWS, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan AWS Account Management Referensi.

Anda dapat mengaktifkan Hub Keamanan untuk akun atau akun individual di organisasi Anda. Di setiap Wilayah, Anda dapat mengakses dan menggunakan Hub Keamanan dengan salah satu cara berikut:

Konsol Hub Keamanan

Konsol Security Hub adalah antarmuka berbasis browser yang dapat Anda gunakan untuk membuat dan mengelola AWS sumber daya. Di konsol ini, Anda dapat mengakses akun, data, dan sumber daya.

API Hub Keamanan

Security Hub API memberi Anda akses terprogram ke akun, data, dan sumber daya Anda. Anda dapat mengirim permintaan HTTPS langsung ke Hub Keamanan.

AWS CLI

Dengan AWS CLI, Anda dapat menjalankan perintah di baris perintah sistem Anda untuk melakukan tugas dan membangun skrip yang melakukan tugas. Dalam beberapa kasus, AWS CLI bisa lebih berguna daripada konsol Hub Keamanan.

AWS SDK

AWS SDK terdiri dari pustaka dan kode sampel untuk berbagai bahasa pemrograman dan platform (C ++, Go, Java, .NET, dan Python). Mereka menyediakan akses terprogram ke Hub Keamanan dan lainnya Layanan AWS dalam bahasa pilihan Anda dan dapat membantu Anda mengelola tugas seperti mengelola kesalahan, permintaan penandatanganan, dan permintaan percobaan ulang.

Konsep Hub Keamanan

Di Security Hub, kami membangun AWS konsep dan terminologi umum dan menggunakan istilah tambahan ini.

Akun

AWS Akun standar yang berisi AWS sumber daya Anda. Masuk AWS dengan AWS akun Anda untuk mengaktifkan Hub Keamanan.

Jika akun Anda terdaftar AWS Organizations, organisasi Anda akan menunjuk akun administrator Hub Keamanan. Akun ini dapat mengaktifkan akun organisasi lain sebagai akun anggota.

Organisasi hanya dapat memiliki satu akun administrator. Akun tidak dapat menjadi akun administrator dan akun anggota secara bersamaan.

Security Hub mendukung akun berikut:

- Akun manajemen organisasi — AWS akun yang mengelola AWS organisasi.
- Akun administrator yang didelegasikan — AWS akun yang mengelola penggunaan Layanan AWS untuk AWS organisasi.
- Akun anggota — AWS akun yang merupakan anggota AWS organisasi.
- Akun mandiri — AWS akun tanpa AWS Organizations diaktifkan.

Akun Administrator

Jenis AWS akun ini dapat melihat temuan untuk akun anggota terkait.

Jenis AWS akun ini menjadi akun administrator ketika akun ditunjuk oleh akun manajemen organisasi sebagai akun administrator Hub Keamanan. Akun administrator Hub Keamanan dapat mengaktifkan akun organisasi apa pun sebagai akun anggota dan juga dapat mengundang akun lain untuk menjadi akun anggota.

Organisasi hanya dapat memiliki satu akun administrator. Akun tidak dapat menjadi akun administrator dan akun anggota secara bersamaan.

Wilayah Agregasi

Wilayah agregasi memungkinkan Anda untuk melihat temuan keamanan dari beberapa Wilayah AWS dalam satu panel kaca.

Wilayah agregasi adalah Wilayah AWS tempat Anda melihat dan mengelola temuan. Temuan digabungkan dalam Wilayah agregasi dari Wilayah terkait. Temuan terbaru direplikasi di seluruh Wilayah.

Di Wilayah agregasi, dasbor dan halaman inventaris menyertakan data dari semua Wilayah yang ditautkan. Halaman otomatisasi hanya dapat digunakan untuk menentukan aturan otomatisasi di wilayah agregasi. Third-party integrasi tiket hanya dapat dikonfigurasi di wilayah agregasi.

Temuan yang diarsipkan

Sebuah temuan dengan status`ARCHIVED`. Temuan ini menunjukkan penyedia temuan atau pelanggan yang menyelidiki temuan percaya temuan itu tidak lagi relevan.

Pencari penyedia dapat mengarsipkan penemuan yang mereka buat. Pelanggan dapat mengarsipkan temuan apa pun yang mereka yakini tidak lagi relevan menggunakan pen BatchUpdateFindingsV2 goperasian API Hub Keamanan atau dengan memperbarui status di konsol Hub Keamanan.

Di konsol Hub Keamanan, pengaturan filter default mengecualikan temuan yang diarsipkan dari pencarian daftar dan tabel. Anda dapat memperbarui filter untuk menyertakan temuan yang diarsipkan. Jika Anda mengambil temuan dengan menggunakan operasi GetFindings V2, operasi mengambil temuan yang diarsipkan dan aktif. Contoh berikut menunjukkan cara mengecualikan temuan yang diarsipkan dalam hasil.

```
{
    "StringFilters":
    [
        {
            "FieldName": "status",
            "Filter":
            {
                "Value": "Archived",
                "Comparison": "EQUALS"
            }
        }
    ]
}
```

Cross-Region agregasi

Agregasi temuan dan sumber daya dari Wilayah terkait ke Wilayah agregasi. Anda dapat melihat semua data Anda dari Wilayah agregasi dan memperbarui temuan dari Wilayah agregasi.

Akun administrator yang didelegasikan

Di AWS Organizations, akun administrator yang didelegasikan untuk layanan dapat mengelola penggunaan layanan untuk organisasi.

Di Hub Keamanan, akun administrator Hub Keamanan juga merupakan akun administrator yang didelegasikan untuk Hub Keamanan. Ketika akun manajemen organisasi pertama kali menunjuk

akun administrator Hub Keamanan, Hub Keamanan memanggil Organisasi untuk menjadikan akun tersebut sebagai akun administrator yang didelegasikan.

Akun manajemen organisasi kemudian harus memilih akun administrator yang didelegasikan sebagai akun administrator Hub Keamanan di semua Wilayah.

Paparan

Eksposur adalah kelemahan yang lebih luas dalam kontrol keamanan, kesalahan konfigurasi, atau area lain yang dapat dieksploitasi oleh ancaman aktif.

Contoh eksposur meliputi:

- Pesawat kontrol yang salah konfigurasi untuk sumber daya.
- Adanya kerentanan perangkat lunak yang memiliki potensi eksploitabilitas tinggi.
- Sumber daya yang dapat diakses publik (jaringan atau API).

Penemuan eksposur

Jenis temuan yang menggambarkan paparan yang ada di lingkungan Anda. Temuan eksposur mencakup sifat dan sinyal. Sinyal dapat mencakup satu atau lebih jenis sifat eksposur. AWS Security Hub menghasilkan temuan eksposur ketika sinyal dari AWS Security Hub CSPM, Amazon Inspector, Amazon GuardDuty, Amazon Macie, atau AWS layanan lain, menunjukkan adanya eksposur. Sumber daya dapat terlibat dalam satu atau lebih temuan eksposur. Jika sumber daya tidak memiliki sifat eksposur atau memiliki sifat yang tidak mencukupi, Security Hub tidak menghasilkan temuan eksposur untuk sumber daya tersebut.

Contoh temuan eksposur adalah: Instans EC2 yang dapat dijangkau dari internet dan memiliki kerentanan perangkat lunak yang memiliki kemungkinan eksploitasi tinggi.

Temuan

Catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Security Hub menghasilkan dan memperbarui temuan melalui korelasi temuan keamanan lainnya. Ini disebut temuan eksposur. Temuan juga dapat berasal dari integrasi dengan produk lain Layanan AWS dan pihak ketiga.

Menemukan konsumsi

Impor temuan ke Security Hub. Menemukan peristiwa konsumsi mencakup temuan baru dan pembaruan untuk temuan yang ada.

Wilayah Terkait

Bila Anda mengaktifkan agregasi lintas wilayah, Wilayah tertaut adalah wilayah yang menggabungkan temuan dan inventaris sumber daya ke Wilayah agregasi.

Di Wilayah yang ditautkan, dasbor dan halaman inventaris hanya berisi temuan untuk itu Wilayah AWS.

Kerangka skema keamanan siber terbuka (OCSF)

Open Cybersecurity Schema Framework (OCSF) adalah upaya kolaboratif sumber terbuka oleh AWS dan mitra terkemuka di industri keamanan siber. OCSF menyediakan skema standar untuk peristiwa keamanan umum, mendefinisikan kriteria pembuatan versi untuk memfasilitasi evolusi skema, dan mencakup proses pemerintahan sendiri untuk produsen dan konsumen log keamanan. Untuk informasi selengkapnya, lihat temuan OCSF di Hub Keamanan.

Akun Anggota

An Akun AWS yang memberikan izin kepada akun administrator untuk melihat dan mengambil tindakan atas temuan mereka. Jenis ini Akun AWS menjadi akun anggota ketika akun administrator Hub Keamanan mengaktifkannya sebagai akun anggota.

Sinyal

Temuan yang berkontribusi pada temuan eksposur. Sinyal dapat disebut sebagai temuan yang berkontribusi. Sinyal dapat berasal dari Security Hub CSPM,, atau lainnya AWS Config Layanan AWS, seperti Amazon Inspector.

Service-linked perekam konfigurasi

Jenis AWS Config perekam yang digunakan untuk merekam data konfigurasi pada sumber daya khusus layanan. Security Hub menggunakan perekam ini dalam pendekatan berbasis peristiwa untuk mendapatkan item konfigurasi sumber daya untuk cakupan analisis eksposur, pelaporan inventaris sumber daya, dan evaluasi kontrol manajemen postur. Kemampuan ini disediakan untuk semua pelanggan Security Hub sebagai bagian dari harga paket Essential. Setelah Anda mengaktifkan Hub Keamanan, perekam konfigurasi terkait layanan berikut akan dibuat di akun Anda:

- Di setiap Akun AWS dan Wilayah AWS, perekam konfigurasi terkait layanan bernama `AWSConfigurationRecorderForSecurityHubAssets` dibuat.
- Untuk jenis sumber daya global, perekam konfigurasi terkait layanan tambahan bernama `AWSConfigurationRecorderForSecurityHubAssetsGlobal` dibuat di us-east-1. Wilayah AWS

- Jika Security Hub dan Security Hub CSPM keduanya diaktifkan di Akun AWS dan Wilayah AWS, perekam konfigurasi terkait layanan bernama dibuat. `AWSConfigurationRecorderForSecurityHubCSPM`

Untuk informasi selengkapnya, lihat Per timbangan untuk perekam konfigurasi terkait layanan dan Merekam sumber daya regional dan global.

Service-linked penganalisis

Penganalisis Akses IAM yang dibuat dan dikelola oleh Security Hub atas nama Anda. Saat Anda mengaktifkan Hub Keamanan, secara otomatis membuat penganalisis akses yang tidak terpakai yang ditautkan ke layanan untuk mengidentifikasi peran IAM, pengguna, kunci akses, dan izin yang belum digunakan dalam periode tampilan balik 90 hari. Alat analisa berjalan di AS Timur (Virginia Utara) karena IAM adalah layanan global. Security Hub mereplikasi temuan akses yang tidak digunakan ke semua Wilayah tempat Anda mengaktifkan Hub Keamanan. Anda tidak perlu mengaktifkan IAM Access Analyzer secara terpisah atau mengambil tindakan tambahan apa pun. Kemampuan ini disediakan untuk semua pelanggan Security Hub sebagai bagian dari harga paket Essential. Anda dapat melihat penganalisis terkait layanan di konsol Penganalisis Akses IAM, tetapi Anda tidak dapat memodifikasi atau menghapusnya saat Hub Keamanan diaktifkan. Security Hub menghapus penganalisis saat Anda menonaktifkan layanan di semua wilayah. Akun AWS Untuk informasi selengkapnya, lihat the section called “Temuan akses yang tidak digunakan”.

Sifat

Penyimpangan keamanan yang menghasilkan temuan eksposur. Jenis sifat termasuk A sumabilitas, Miskonfigurasi, Jangkauan, Data Sensitif, dan Ker entanan. Suatu sifat dikaitkan dengan satu sinyal, dan sinyal dapat mengandung banyak sifat. Misalnya, kontrol CSPM Security Hub menunjukkan kebijakan yang dikelola pelanggan memungkinkan kontrol akses administratif. Sinyal ini mengandung sifat salah konfigurasi.

Penemuan akses yang tidak digunakan

Temuan yang mengidentifikasi peran IAM, pengguna, kunci akses, atau kumpulan izin yang belum digunakan dalam periode lookback 90 hari. Security Hub menghasilkan temuan akses yang tidak digunakan menggunakan Penganalisis Akses IAM yang ditautkan ke layanan. Ada empat jenis temuan akses yang tidak digunakan: peran IAM yang tidak digunakan, kunci akses pengguna IAM yang tidak digunakan, kata sandi pengguna IAM yang tidak digunakan, dan izin yang tidak digunakan.

AWS Penaksir Biaya Hub Keamanan

Penaksir biaya Hub Keamanan adalah fitur konsol yang memberikan perkiraan kemampuan Hub Keamanan di seluruh AWS lingkungan Anda. Penaksir biaya menunjukkan kepada Anda berapa biaya layanan individual Anda di AWS Security Hub CSPM, Amazon Inspector, dan Amazon GuardDuty dan berapa perkiraan biaya Anda di Security Hub dengan paket harga yang disederhanakan dari Security Hub. Anda dapat menyesuaikan perkiraan penggunaan dan jumlah sumber daya agar sesuai dengan AWS penggunaan Anda untuk meningkatkan akurasi perkiraan Anda. Penaksir biaya tersedia di semua wilayah di mana Security Hub tersedia.

Penaksir biaya memperkirakan biaya bulanan untuk kemampuan keamanan menggunakan dua model penetapan harga:

- Harga layanan individual — Bayar untuk setiap fitur keamanan secara terpisah (GuardDuty, Amazon Inspector, Security Hub CSPM).
- Harga Security Hub yang disederhanakan — Penetapan harga terpadu di 3 paket harga, paket penting dengan harga per sumber daya, analisis ancaman dengan harga log per peristiwa dan per GB, dan pemindaian Kode Lambda dengan harga per sumber daya.

Penaksir menggunakan AWS Cost Explorer data jika tersedia. Ketika data Cost Explorer tidak tersedia, Anda dapat memasukkan data penggunaan secara manual. Perkiraan biaya didasarkan pada penggunaan yang diamati dan disediakan pengguna, dan informasi harga publik. Perkiraan mungkin tidak mencerminkan diskon perusahaan.

Manfaat utama dari estimator biaya meliputi:

- Lihat bagaimana biaya dengan harga terpadu, saat mengaktifkan Hub Keamanan, dibandingkan dengan biaya dengan layanan individual tanpa mengaktifkan Hub Keamanan
- Perkirakan biaya sebelum mengaktifkan kemampuan
- Sesuaikan parameter penggunaan untuk memodelkan skenario yang berbeda
- Ekspor perkiraan sebagai PDF untuk tinjauan pemangku kepentingan

Akses berdasarkan jenis akun

> **Note**
>
> Untuk administrator yang didelegasikan dan akun anggota, penaksir biaya terbuka dalam mode edit secara default, memungkinkan Anda untuk segera memasukkan data penggunaan. Akun manajemen dan akun mandiri terbuka dalam mode tampilan saat data Cost Explorer tersedia.

Fitur ini secara otomatis mengambil informasi tentang penggunaan masa lalu aktual untuk memperkirakan biaya untuk jenis akun tertentu. Lihat tabel berikut untuk detail tentang setiap jenis akun dan data yang tersedia untuk setiap jenis akun.

Izin akses berdasarkan jenis akun

Jenis Akun	Data Penjelajah Biaya	Entri Data	Lingkup
Akun Manajemen (MA)	Auto-populated	Tersedia penggantian manual	Organization-wide
Administrator Delegasi (DA)	Auto-populated melalui peran lintas akun*	Tersedia penggantian manual	Organization-wide
Akun Anggota	Auto-populated melalui peran lintas akun*	Tersedia penggantian manual	Organization-wide
Akun Mandiri (SA)	Auto-populated	Tersedia penggantian manual	Akun tunggal

* Memerlukan konfigurasi peran IAM lintas akun di akun manajemen. Lihat Menyiapkan akses lintas akun bagian di bawah ini.

Prasyarat

Izin IAM yang diperlukan

Untuk menggunakan semua kemampuan penaksir biaya, prinsipal IAM Anda harus memiliki izin berikut:

Izin IAM yang diperlukan untuk Penaksir Biaya

Operasi API	Layanan	Tujuan
`ce:GetCostAndUsage`	AWS Penjelajah Biaya	Mengambil data penggunaan dan biaya historis
`pricing:GetProducts`	AWS Harga	Dapatkan harga terkini
`organizations:ListAccounts`	AWS Organisasi	Hitung akun dalam organisasi
`organizations:DescribeOrganization`	AWS Organisasi	Tentukan jenis akun
`securityhub:ListOrganizationAdminAccounts`	Hub Keamanan	Daftar akun admin organisasi
`iam:GetRole`	IAM	Periksa keberadaan peran lintas akun (Hanya akun manajemen) *
`sts:AssumeRole`	IAM	Mengasumsikan peran lintas akun (hanya administrator/Member akun yang didelegasikan) **

* Diperlukan hanya bagi pengguna Akun Manajemen untuk memverifikasi status peran lintas akun.

** Diperlukan hanya untuk akun Administrator Delegasi dan Anggota Organisasi yang menggunakan akses lintas akun.

Persyaratan tambahan

Cost Explorer

Harus diaktifkan untuk populasi data otomatis (penundaan pemrosesan 24 jam setelah pengaktifan).

Menyiapkan akses lintas akun

Administrator yang didelegasikan dan akun anggota dapat mengakses AWS Cost Explorer data seluruh organisasi dari akun manajemen dengan mengonfigurasi peran IAM lintas akun. Konfigurasi ini memungkinkan akun ini untuk melihat data penggunaan aktual tanpa beralih ke akun manajemen.

Prasyarat

Item dan informasi berikut diperlukan sebelum menyiapkan akses lintas akun untuk penaksir biaya:

- Akun manajemen harus AWS Cost Explorer diaktifkan.
- Izin IAM untuk membuat peran di akun manajemen.
- Pengetahuan tentang administrator yang didelegasikan atau ID akun anggota yang akan diberikan akses lintas akun.

Langkah-langkah penyiapan

Penaksir biaya menyediakan instruksi pengaturan terpandu langsung di konsol. Untuk mengakses instruksi, navigasikan ke halaman penaksir biaya di https://console.aws.amazon.com/securityhub/v2/home #/CostEstimator di akun manajemen organisasi Anda. Temukan bagian Cross-account akses dan ikuti langkah-langkah yang diuraikan untuk mengatur peran lintas akun.

Konfigurasi peran

Akses lintas akun untuk penaksir biaya memerlukan pengaturan peran IAM dengan kebijakan kepercayaan dan kebijakan izin. Peran lintas akun harus dibuat di akun manajemen dengan konfigurasi berikut:

Nama peran (nama yang tepat diperlukan) — AwsSecurityHubCostEstimatorCrossAccountRole

Kebijakan kepercayaan yang direkomendasikan:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
            "AWS": "arn:aws:iam::{ACCOUNT_ID}:role/{ROLE_NAME}"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Edit kebijakan dengan mengganti nilai-nilai berikut dalam contoh kebijakan:

- Ganti *{ACCOUNT_ID}* dengan administrator yang didelegasikan atau ID akun anggota yang Anda berikan akses lintas akun.
- Ganti *{ROLE_NAME}* dengan nama peran IAM di administrator atau akun anggota yang didelegasikan yang Anda berikan aksesnya.

Kebijakan izin yang disarankan:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ce:GetCostAndUsage",
            "Resource": "*"
        }
    ]
}
```

Note

Kebijakan kepercayaan membatasi akses ke akun dan peran tertentu. Hanya prinsipal IAM yang ditentukan yang dapat mengambil peran ini, mencegah akses yang tidak sah.

Verifikasi

Setelah membuat peran di akun manajemen gunakan langkah-langkah berikut untuk mengonfirmasi pengaturan berfungsi.

1. Masuk ke administrator atau akun anggota yang didelegasikan.
2. Arahkan ke penaksir biaya Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home #/costEstimator
3. Halaman harus secara otomatis:

    a. Mendeteksi akun manajemen di organisasi Anda.

    b. Asumsikan peran lintas akun.

    c. Muat data Cost Explorer dengan penggunaan di seluruh organisasi.

Jika berhasil, data penggunaan aktual muncul sebagai pengganti bidang entri manual.

Pemecahan masalah

Bagian ini mencakup masalah umum dan solusi yang dapat terjadi saat menyiapkan akses lintas akun.

Data penggunaan organisasi tidak tersedia untuk akun ini

Peringatan ini menunjukkan peran lintas akun tidak dapat diakses. Kemungkinan penyebab peringatan ini adalah:

1. Peran tidak ada: Akun manajemen belum membuat peran.

    - Solusi: Hubungi administrator akun manajemen Anda untuk membuat peran menggunakan panduan penyiapan.
2. Ketidakcocokan nama peran: Nama peran tidak cocok persis.

    - Solusi: Verifikasi nama peran adalah`AwsSecurityHubCostEstimatorCrossAccountRole`.
3. Kebijakan kepercayaan salah: Kebijakan kepercayaan tidak mengizinkan akun Anda untuk mengambil peran tersebut.

    - Solusi: Verifikasi kebijakan kepercayaan termasuk ID akun dan nama peran Anda.
4. AssumeRole Izin hilang: Prinsip IAM Anda kurang. `sts:AssumeRole`

- Solusi: Hu bungi administrator Anda untuk menambahkan `sts:AssumeRole` izin.

Untuk melihat petunjuk penyiapan terperinci: Pilih Lihat instruksi dalam peringatan untuk membuka modal dengan panduan langkah demi langkah dan templat kebijakan.

Solusi: Anda masih dapat menggunakan Penaksir Biaya dengan memasukkan nilai penggunaan secara manual dalam mode edit.

Menggunakan penaksir biaya

Mengakses estimator biaya

Untuk mengakses Penaksir Biaya dari halaman arahan Hub Keamanan

1. Masuk ke AWS akun Anda dengan kredentif AWS akun administrator manajemen atau administrator yang didelegasikan. Buka konsol Hub Keamanan di wilayah us-east-1 di. https://console.aws.amazon.com/securityhub/v2/home
2. Di halaman arahan, cari kartu Harga.
3. Pilih Perkiraan biaya.

Untuk mengakses Penaksir Biaya selama langkah pengaktifan dan konfigurasi Hub Keamanan

1. Temukan Harga di kartu Hub Keamanan baru di antarmuka onboarding.
2. Pilih Lihat perkiraan.

Untuk mengakses penaksir biaya dari GuardDuty, Amazon Inspector, atau konsol CSPM Security Hub

1. Arahkan ke dasbor layanan atau halaman ringkasan.
2. Pilih Bandingkan harga di kartu informasi harga.

Memahami antarmuka penaksir biaya

Tata letak halaman

Halaman Penaksir Biaya berisi tiga bagian utama:

- Bagian ikh tisar - Menjelaskan manfaat manajemen keamanan terpadu dan pengoptimalan biaya.
- Informasi harga - Panel yang dapat diperluas dengan kategori kemampuan dan tingkatan harga.
- Tabel perbandingan harga — perbandingan Side-by-side biaya dengan detail kemampuan.

Tabel perbandingan harga

Header tabel mencakup kontrol view/edit mode dan opsi reset. Tabel menampilkan biaya dalam dua kolom:

- Layanan individu — Biaya saat ini atau perkiraan untuk layanan keamanan terpisah.
- Security Hub — Perkiraan biaya menggunakan model penetapan harga yang disederhanakan.

Wilayah harga

Kolom pertama menampilkan informasi konteks harga, termasuk catatan bahwa perkiraan menggunakan harga us-east-1 untuk perhitungan. Lencana menunjukkan bahwa diskon perusahaan tidak termasuk dalam perkiraan.

Melihat perkiraan biaya

Saat menggunakan penaksir biaya, Anda dapat melihat, mengedit, mengatur ulang, dan mengekspor perkiraan.

Penaksir biaya terbuka dalam mode tampilan secara default.

Untuk melihat perkiraan biaya

1. Akses Penaksir Biaya menggunakan salah satu metode yang dijelaskan diMengakses estimator biaya.
2. Tinjau total biaya bulanan di baris ringkasan.
3. Tinjau grup kemampuan dan rincian biaya terperinci mereka.
4. Pilih nama kemampuan untuk melihat deskripsi di popover.

Sumber data dalam mode tampilan

Penaksir menampilkan data dari berbagai sumber, ditunjukkan oleh label:

- Default — Data dari AWS Cost Explorer (30 hari terakhir).
- $-/bln — Data biaya tidak tersedia (ditampilkan saat akses Cost Explorer tidak tersedia).
- Penggunaan kustom — User-entered nilai.
- Tidak diaktifkan — Menampilkan saat izin Cost Explorer tidak ada.

Account-specific perilaku

Berikut ini menjelaskan bagaimana penaksir biaya berfungsi di berbagai jenis akun dan konfigurasi.

Administrator yang didelegasikan dan akun anggota

Dengan akses lintas akun dikonfigurasi:

- Data Cost Explorer tersedia dengan penggunaan di seluruh organisasi.
- Terbuka dalam mode tampilan secara default (sama seperti akun manajemen). Anda dapat beralih ke mode edit untuk mengubah perkiraan.

Tanpa akses lintas akun dikonfigurasi:

- Peringatan ditampilkan: “Data penggunaan organisasi tidak tersedia untuk akun ini”.
- Terbuka dalam mode edit secara default untuk entri manual.
- Pilih Lihat instruksi dalam peringatan untuk panduan penyiapan.

Akun manajemen

Dengan peran lintas akun yang dibuat:

- bagian “Cross-account akses” menunjukkan status yang dikonfigurasi.
- Menampilkan kebijakan yang direkomendasikan untuk verifikasi.
- Menyediakan tautan untuk melihat peran di konsol IAM.

Tanpa peran lintas akun yang dibuat:

- bagian “Cross-account akses” menampilkan panduan pengaturan.
- Menyediakan petunjuk langkah demi langkah dengan kebijakan yang telah diisi sebelumnya.

- Tautan langsung ke konsol IAM untuk pembuatan peran.

Tidak dapat memverifikasi status peran:

- Jika tidak ada izin untuk meneleponiam:GetRole, konsol tidak dapat menentukan apakah Anda telah membuat peran yang diperlukan.
- Menunjukkan “Tidak dapat memverifikasi” dengan pesan kesalahan yang sesuai.

Akun mandiri

Tanpa peran lintas akun yang dibuat:

- Tidak ada perubahan pada perilaku yang ada.
- Data Cost Explorer tersedia saat diaktifkan.
- Terbuka dalam mode tampilan secara default.

Mengedit nilai penggunaan

Mode edit memungkinkan Anda untuk mengubah nilai dimensi dan melihat pembaruan biaya real-time.

Untuk mengedit nilai penggunaan

1. Pilih Edit di header tabel.
2. Masukkan nilai di bidang input dimensi.
3. Lihat biaya yang diperbarui secara otomatis.
4. Pilih Lihat untuk kembali ke mode tampilan.

> **Important**
>
> - Pengeditan tidak disimpan saat Anda meninggalkan halaman penaksir biaya
> - Perkiraan yang dimodifikasi menggunakan harga us-east-1 (Virginia Utara) dan tidak termasuk diskon perusahaan
> - Mengedit dalam mode “Tampilkan hanya biaya saat ini” secara otomatis beralih kembali ke mode perkiraan

Mengatur ulang estimator

Tindakan ini menghapus semua nilai kustom dan memuat ulang data default dari Cost Explorer.

Untuk mengatur ulang semua nilai ke default

1. Pilih Reset di header tabel.
2. Pada dialog konfirmasi, pilih Reset.

Mengekspor perkiraan

Sementara di estimator biaya, data untuk perkiraan Anda dapat diekspor ke file PDF.

Untuk mengekspor perkiraan biaya

1. Pastikan Anda berada dalam mode tampilan.
2. Pilih Unduh PDF di header halaman.

PDF diunduh secara otomatis dengan nama file:`SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf`.

Pemecahan masalah

Bagian ini mencakup masalah umum dan solusi yang dapat terjadi saat menggunakan penaksir biaya

Tidak ada data Cost Explorer yang tersedia

Masalah

Peringatan menampilkan “Tidak ada data biaya tersedia untuk akun Anda”.

Solusi berdasarkan jenis akun

Solusinya tergantung pada jenis akun Anda:

Solusi untuk data Cost Explorer yang hilang

Jenis Akun	Solusi
Akun Manajemen	Aktifkan Cost Explorer dan tunggu 24 jam untuk pemrosesan data

Jenis Akun	Solusi
Administrator yang Delegasi	Hubungi administrator Akun Manajemen untuk meminta akses
Akun Anggota	Hubungi Akun Manajemen atau Administrator Delegasi untuk akses
Akun Mandiri	Aktifkan Cost Explorer dan tunggu 24 jam untuk pemrosesan data

Solusi

Masukkan nilai kustom dalam mode edit.

Cross-account akses tidak berfungsi

Masalah

Administrator atau akun anggota yang didelegasikan menampilkan peringatan “Data penggunaan organisasi tidak tersedia untuk akun ini”.

Tinjau penyebab umum berikut dan solusinya:

Cross-account peran tidak ada di akun manajemen

Hubungi administrator Akun Manajemen untuk membuat peran. Penaksir biaya menyediakan petunjuk penyiapan terpandu untuk pengguna akun manajemen.

Nama peran tidak cocok persis

Nama peran yang diperlukan:`AwsSecurityHubCostEstimatorCrossAccountRole`. Verifikasi nama peran di konsol IAM cocok persis (peka huruf besar/kecil).

Kebijakan kepercayaan tidak mengizinkan akun Anda

Verifikasi prinsip kebijakan kepercayaan mencakup ID akun dan nama peran Anda. Format: `arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}`.

Kehilangan AssumeRole izin

Pastikan kepala sekolah IAM Anda memiliki `sts:AssumeRole` izin. Hubungi AWS administrator Anda untuk menambahkan izin ini.

Solusi:

Masukkan nilai kustom dalam mode edit untuk memperkirakan biaya secara manual tanpa data Cost Explorer.

Mendapatkan instruksi terperinci

- Pilih Lihat instruksi dalam peringatan untuk membuka modal dengan:
  - Step-by-step panduan penyiapan
  - Pre-populated templat kebijakan
  - Kiat pemecahan masalah khusus untuk kesalahan Anda

Kesalahan izin

Masalah

Kesalahan “Akses ditolak” untuk operasi API tertentu.

Untuk mengatasi kesalahan izin

1. Perhatikan operasi yang ditolak dari pesan kesalahan (misalnya,`ce:GetCostAndUsage`).
2. Pilih Sal in untuk menyalin detail kesalahan.
3. Kirim rincian kesalahan ke AWS administrator Anda.
4. Minta izin IAM yang diperlukan yang tercantum diIzin IAM yang diperlukan.

> **Note**
>
> Anda masih dapat menggunakan mode edit untuk memasukkan nilai manual saat izin hilang, kecuali ketika akses Pricing API ditolak (mencegah semua perkiraan biaya).

Kemampuan menunjukkan “Tidak diaktifkan”

Masalah

Kemampuan menampilkan status “Tidak diaktifkan”.

Penjelasan

Status ini muncul ketika Anda memiliki akses Cost Explorer tetapi kemampuan saat ini tidak aktif. Jika Anda melihat $-/bln sebagai gantinya, ini menunjukkan bahwa data Cost Explorer tidak tersedia untuk jenis akun Anda.

Untuk melihat perkiraan biaya

1. Pilih Edit untuk masuk ke mode edit.
2. Masukkan nilai dimensi untuk kemampuan.
3. Lihat perkiraan biaya yang diperbarui.

Kemampuan menunjukkan “Tidak berlaku”

Masalah

Kemampuan menampilkan “Tidak berlaku” di kolom Layanan individual.

Penjelasan

Kemampuan ini hanya tersedia melalui penetapan harga Security Hub yang disederhanakan, bukan sebagai layanan mandiri.

Biaya yang dimodifikasi tidak cocok dengan Cost Explorer

Masalah

Biaya yang diedit berbeda dari nilai Cost Explorer asli.

Penjelasan

Perkiraan yang dimodifikasi menggunakan tarif harga us-east-1 (Virginia Utara) dan tidak termasuk diskon perusahaan. Data Cost Explorer mencerminkan biaya aktual dengan diskon yang berlaku.

Catatan penting

- Perkiraan didasarkan pada penggunaan yang diamati dan disediakan pengguna, dan informasi harga publik — Biaya aktual mungkin bervariasi berdasarkan pola penggunaan dan perjanjian perusahaan
- 30 hari melihat ke belakang — Data Cost Explorer mencerminkan penggunaan 30 hari terakhir
- Wilayah penetapan harga - Semua perkiraan menggunakan tarif us-east-1 (Virginia Utara)

- Tidak berdampak pada pengaturan — Perubahan pada estimator tidak memengaruhi Hub Keamanan atau konfigurasi layanan Anda saat ini
- Diskon perusahaan — Perkiraan yang dimodifikasi tidak termasuk diskon perusahaan; hanya data Cost Explorer yang mencerminkan biaya diskon aktual
- Penyegaran data - Pembaruan data Cost Explorer setiap hari; refresh halaman untuk melihat data terbaru

Informasi Terkait

- AWS Harga Security Hub
- AWS Panduan Pengguna Cost Explorer
- AWS Referensi API Harga
- Mengaktifkan Hub Keamanan

Mengaktifkan Hub Keamanan

Anda dapat mengaktifkan Hub Keamanan untuk apa pun Akun AWS. Bagian dokumentasi ini menjelaskan semua langkah yang diperlukan untuk mengaktifkan Hub Keamanan untuk AWS Organisasi, atau akun mandiri.

Untuk demonstrasi singkat tentang cara mengaktifkan Hub Keamanan, tonton video berikut: Panduan dan Demo Onboarding Hub Keamanan.

Aktifkan Hub Keamanan untuk AWS Organisasi

Bagian ini mencakup tiga langkah:

- Pada Langkah 1, akun manajemen AWS organisasi menunjuk administrator yang didelegasikan untuk AWS Organisasi mereka, membuat kebijakan administrator yang didelegasikan, dan secara opsional mengaktifkan Hub Keamanan untuk akun mereka sendiri.
- Pada Langkah 2, administrator yang didelegasikan untuk organisasi mengaktifkan Hub Keamanan untuk akun mereka sendiri.
- Pada Langkah 3, administrator yang didelegasikan untuk organisasi mengonfigurasi semua akun anggota di organisasi, untuk Hub Keamanan, dan layanan keamanan lain yang didukung.

Langkah 1. Mendelegasikan akun administrator dan secara opsional mengaktifkan Hub Keamanan di AWS akun manajemen organisasi

> **Note**
>
> Selesaikan langkah ini di satu Wilayah dari akun manajemen organisasi.

Saat menetapkan akun administrator yang didelegasikan untuk Hub Keamanan, akun yang dapat Anda pilih untuk administrator yang didelegasikan bergantung pada cara Anda mengonfigurasi administrator yang didelegasikan untuk Security Hub CSPM. Jika Anda telah mengonfigurasi administrator yang didelegasikan untuk Security Hub CSPM, dan akun tersebut bukan akun manajemen organisasi, maka akun tersebut secara otomatis ditetapkan sebagai administrator yang didelegasikan Hub Keamanan dan akun yang berbeda tidak dapat dipilih. Jika akun administrator yang didelegasikan untuk Security Hub CSPM ditetapkan sebagai akun manajemen organisasi atau tidak disetel sama sekali, Anda dapat memilih akun yang akan ditetapkan sebagai akun administrator delegasi Hub Keamanan Anda, kecuali untuk akun manajemen organisasi.

Untuk informasi tentang menunjuk administrator yang didelegasikan di Hub Keamanan, lihat Menunjuk akun administrator yang didelegasikan di Hub Keamanan. Untuk informasi tentang membuat kebijakan administrator yang didelegasikan di Hub Keamanan, lihat Membuat kebijakan administrator yang didelegasikan di Hub Keamanan.

Untuk menunjuk administrator untuk Hub Keamanan

1. Masuk ke AWS akun Anda dengan kredensional akun manajemen AWS organisasi Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari beranda Hub Keamanan, pilih Hub Keamanan, lalu pilih Memulai.
3. Di bagian Administrator yang di delegasikan, pilih akun administrator berdasarkan opsi yang disediakan. Sebagai praktik terbaik, gunakan administrator yang didelegasikan yang sama di seluruh layanan keamanan untuk tata kelola yang konsisten.
4. Pilih kotak centang Akses tepercaya. Memilih opsi ini memberi akun administrator yang didelegasikan kemampuan untuk mengonfigurasi kemampuan tertentu, seperti GuardDuty Perlindungan Malware, pada akun anggota. Jika Anda menghapus centang pada opsi ini, Security Hub tidak dapat mengaktifkan fitur-fitur ini atas nama Anda dan Anda harus mengaktifkannya secara langsung melalui layanan yang terkait dengan fitur tersebut.
5. (Opsional) Untuk pengaktifan Akun, pilih kotak untuk mengaktifkan Hub Keamanan untuk akun Anda AWS .
6. Untuk Kebijakan administrator yang di delegasikan, pilih salah satu opsi berikut untuk menambahkan pernyataan kebijakan.

    a. (Opsi 1) Pilih Per barui ini untuk saya. Pilih kotak di bawah pernyataan kebijakan untuk mengonfirmasi bahwa Hub Keamanan secara otomatis membuat kebijakan delegasi yang memberikan semua izin yang diperlukan kepada administrator yang didelegasikan.

    b. (Opsi 2) Pilih Saya ingin melampirkan ini secara manual. Pilih Sal in dan lampirkan. Di AWS Organizations konsol, di bawah Administrator yang di delegasikan untuk AWS Organizations, pilih Delegasikan, dan tempel kebijakan sumber daya di editor kebijakan delegasi. Pilih Buat Kebijakan. Buka tab tempat Anda berada di konsol Hub Keamanan.
7. Pilih Konfigurasikan

Langkah 2. Aktifkan Hub Keamanan di akun administrator yang didelegasikan

Akun administrator yang didelegasikan menyelesaikan langkah ini. Setelah akun manajemen AWS Organisasi menunjuk administrator yang didelegasikan untuk organisasi mereka, administrator yang didelegasikan harus mengaktifkan Hub Keamanan untuk akun mereka sendiri sebelum mengaktifkan untuk seluruh AWS Organisasi.

Untuk mengaktifkan Hub Keamanan di akun administrator yang didelegasikan

1. Masuk ke AWS akun Anda dengan kredensional administrator yang didelegasikan. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari beranda Hub Keamanan, pilih Memulai.
3. Bagian kemampuan keamanan menguraikan kemampuan yang secara otomatis diaktifkan dan disertakan dalam harga dasar per sumber daya Hub Keamanan.
4. (Opsional) Untuk Tag, tentukan apakah akan menambahkan pasangan kunci-nilai ke pengaturan akun.
5. Pilih Aktifkan Hub Keamanan untuk menyelesaikan pengaktifan Hub Keamanan.
6. (Direkomendasikan) dari popup pilih Konfigurasikan organisasi saya dan lanjutkan ke Langkah 3.

Langkah 3. Membuat kebijakan yang mengaktifkan Hub Keamanan di semua akun anggota

Setelah mengaktifkan Hub Keamanan di akun administrator yang didelegasikan untuk organisasi, Anda perlu membuat kebijakan yang menentukan layanan dan kemampuan mana yang diaktifkan di akun anggota organisasi. Untuk informasi selengkapnya, lihat Mengaktifkan konfigurasi dengan jenis kebijakan.

Setelah Anda mengaktifkan Hub Keamanan, sumber daya berikut dibuat di akun Anda:

- Peran terkait layanan disebut. AWSServiceRoleForSecurityHubV2
- Service-linked perekam konfigurasi. Lihat Service-linked perekam dalam dokumentasi konsep Hub Keamanan untuk detail selengkapnya.
- Penganalisis terkait layanan. Lihat Service-linked penganalisis dalam dokumentasi konsep Hub Keamanan untuk detail selengkapnya.

Aktifkan Hub Keamanan di akun mandiri

Prosedur ini menjelaskan cara mengaktifkan Hub Keamanan di akun mandiri. Akun mandiri adalah akun Akun AWS yang belum mengaktifkan AWS organisasi.

Untuk mengaktifkan Hub Keamanan di akun mandiri

1. Masuk ke AWS akun Anda dengan kredenSIAL akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari beranda Hub Keamanan, pilih Memulai.
3. Di bagian Kemampuan keamanan, lakukan salah satu hal berikut:
   a. (Opsi 1) Pilih Aktifkan semua kemampuan. Ini mengaktifkan semua kemampuan penting Hub Keamanan, analisis ancaman, dan kemampuan tambahan.
   b. (Opsi 2) Pilih Ku stomisasi kemampuan. Pilih kemampuan untuk diaktifkan dari bagian Manajemen keamanan, Analisis ancaman, dan Manajemen kerentanan. Anda tidak dapat membatalkan pilihan kemampuan apa pun yang merupakan bagian dari kemampuan paket penting Hub Keamanan.
4. Di bagian Wil ayah, pilih Aktifkan semua Wilayah atau Aktifkan Wilayah tertentu. Jika Anda memilih Aktifkan semua Wilayah, Anda dapat menentukan apakah akan secara otomatis mengaktifkan Wilayah baru. Jika Anda memilih Aktifkan Wilayah tertentu, Anda harus memilih Wilayah mana yang ingin Anda aktifkan.
5. (Opsional) Untuk tag Sumber daya, tambahkan tag sebagai pasangan kunci-nilai untuk membantu Anda mengidentifikasi konfigurasi dengan mudah.
6. Pilih Aktifkan Hub Keamanan.

Setelah Anda mengaktifkan Hub Keamanan, sumber daya berikut dibuat di setiap akun tempat Anda mengaktifkan layanan:

- Peran terkait layanan disebut. AWSServiceRoleForSecurityHubV2
- Service-linked perekam konfigurasi. Lihat Service-linked perekam dalam dokumentasi konsep Hub Keamanan untuk detail selengkapnya.
- Penganalisis terkait layanan. Lihat Service-linked penganalisis dalam dokumentasi konsep Hub Keamanan untuk detail selengkapnya.

Menunjuk administrator yang didelegasikan di Hub Keamanan

Di akun manajemen AWS organisasi, Anda dapat menunjuk administrator yang didelegasikan untuk organisasi Anda. Sebagai praktik terbaik, gunakan administrator yang didelegasikan yang sama di seluruh layanan keamanan untuk tata kelola yang konsisten.

Prosedur dalam topik ini menjelaskan cara menunjuk administrator yang didelegasikan di Hub Keamanan. Ini mengasumsikan Anda sebelumnya mengaktifkan Hub Keamanan tetapi tidak menunjuk administrator yang didelegasikan selama alur kerja pengaktifan.

Pertimbangan-pertimbangan

Pertimbangkan hal berikut saat menunjuk administrator yang didelegasikan di Hub Keamanan:

- Akun manajemen AWS organisasi dapat menetapkan dirinya sebagai administrator yang didelegasikan di Security Hub CSPM, tetapi tidak dapat menunjuk dirinya sebagai administrator yang didelegasikan di Hub Keamanan. Dalam skenario ini, akun manajemen harus menunjuk yang lain Akun AWS sebagai administrator yang didelegasikan di Hub Keamanan.
- Jika akun manajemen AWS organisasi menunjuk administrator yang didelegasikan di Security Hub CSPM, administrator yang didelegasikan secara otomatis menjadi administrator yang didelegasikan di Hub Keamanan. Dalam skenario ini, Hub Keamanan hanya mengiz Akun AWS inkan khusus ini berfungsi sebagai administrator yang didelegasikan.

> **Note**
>
> Menghapus administrator yang didelegasikan melalui konsol CSPM Security Hub, konsol Hub Keamanan, atau AWS Organizations API menghapusnya dari kedua layanan. Ketika administrator yang didelegasikan dihapus dari CSPM Hub Keamanan, Konfigurasi Pusat secara otomatis memilih keluar.

Menunjuk administrator yang didelegasikan setelah mengaktifkan Hub Keamanan

Prosedur ini untuk menyelesaikan akun manajemen AWS organisasi. Ini mengasumsikan akun manajemen AWS organisasi yang sebelumnya diaktifkan Hub Keamanan tetapi tidak menunjuk administrator yang didelegasikan selama alur kerja pengaktifan.

> **Note**
>
> Setelah menyelesaikan prosedur ini, Anda harus membuat kebijakan yang mengizinkan administrator yang didelegasikan untuk organisasi Anda mengonfigurasi Hub Keamanan dan melakukan tindakan tertentu di AWS Organizations. Untuk informasi selengkapnya, lihat Membuat kebijakan administrator yang didelegasikan di Hub Keamanan.

Untuk menunjuk administrator yang didelegasikan di Hub Keamanan

1. Masuk ke AWS akun Anda dengan kredensional akun manajemen organisasi Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Umum.
3. Di Administrator yang dideleg asikan, pilih Konfigurasi. Pilih salah satu yang disediakan Akun AWS, atau masukkan Akun AWS nomor 12 digit untuk Akun AWS yang ingin Anda tetapkan sebagai administrator yang didelegasikan untuk organisasi Anda. Pilih Simpan.

Membuat kebijakan administrator yang didelegasikan di Hub Keamanan

Akun manajemen AWS organisasi dapat membuat kebijakan yang memungkinkan administrator yang didelegasikan untuk mengonfigurasi Hub Keamanan dan melakukan tindakan tertentu di dalamnya AWS Organizations. Prosedur dalam topik ini menjelaskan cara membuat kebijakan. Saat menyelesaikan prosedur, Anda dapat mengizinkan Hub Keamanan membuat kebijakan untuk Anda atau membuat kebijakan secara manual. Izinkan Hub Keamanan membuat kebijakan kecuali Anda ingin menyesuaikannya untuk kasus penggunaan tertentu.

Selesaikan prosedur ini hanya jika akun manajemen organisasi mengaktifkan Hub Keamanan dan menunjuk administrator yang didelegasikan, tetapi melewatkan pembuatan kebijakan selama alur kerja pengaktifan. Untuk informasi tentang cara memperbarui kebijakan ini, lihat Memper barui kebijakan delegasi berbasis sumber daya dengan AWS Organizations di Panduan AWS Organizations Pengguna.

> **Note**
>
> Setelah Anda menyelesaikan prosedur ini, administrator yang didelegasikan dapat membuat kebijakan untuk mengelola akun anggota di organisasi Anda. Untuk informasi selengkapnya, lihat Membuat kebijakan sebagai administrator yang didelegasikan untuk mengelola akun anggota.

Untuk membuat kebijakan administrator yang didelegasikan

1. Masuk ke AWS akun Anda dengan kredensional akun manajemen organisasi Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Umum.

3. Untuk Kebijakan administrator yang di delegasikan, lakukan salah satu hal berikut:

   - Pilih Buat kebijakan. Pilih kotak di bawah pernyataan kebijakan untuk mengonfirmasi bahwa Hub Keamanan secara otomatis membuat kebijakan delegasi yang memberikan semua izin yang diperlukan kepada administrator yang didelegasikan.
   - Buka kebijakan. Pilih Sal in dan lampirkan. Di AWS Organizations konsol, di bawah Administrator yang di delegasikan untuk AWS Organizations, pilih Delegasikan, dan tempel kebijakan sumber daya di editor kebijakan delegasi. Pilih Buat Kebijakan. Buka tab tempat Anda berada di konsol Hub Keamanan, dan pilih Konfigurasi.

Mengelola konfigurasi akun anggota di AWS Organisasi

Administrator yang didelegasikan untuk AWS Organisasi dapat mengonfigurasi kemampuan keamanan di seluruh akun anggota dan Wilayah. Tersedia dua jenis konfigurasi: Kebijakan dan Pener apan. Kebijakan menghasilkan kebijakan AWS Organisasi untuk akun dan Wilayah untuk Hub AWS Keamanan dan Amazon Inspector. Penerapan adalah tindakan satu kali untuk mengaktifkan kemampuan keamanan di seluruh akun dan Wilayah yang dipilih untuk Amazon GuardDuty dan AWS Security Hub CSPM. Tidak seperti kebijakan, Anda tidak dapat melihat atau mengedit penerapan dan penerapan tidak berlaku untuk akun yang baru diaktifkan. Sebagai alternatif, fitur pengaktifan otomatis untuk akun anggota baru tersedia di Amazon GuardDuty dan AWS Security Hub CSPM.

Katalog konfigurasi Hub Keamanan

Katalog konfigurasi Hub Keamanan menawarkan beberapa opsi untuk membantu mengonfigurasi akun AWS Organisasi Anda untuk kemampuan keamanan yang disediakan oleh Hub Keamanan.

Berikut ini adalah opsi yang tersedia di katalog konfigurasi Hub Keamanan.

Hub Keamanan (kemampuan penting dan tambahan)

Ini adalah konfigurasi yang disarankan untuk digunakan untuk Hub Keamanan.

Jenis: Kebijakan dan Penerapan

Deskripsi: Konfigurasi ini mengaktifkan manajemen keamanan penting, manajemen postur, analisis ancaman, dan kemampuan manajemen kerentanan di Security Hub. Secara opsional memungkinkan kemampuan tambahan.

Analisis ancaman dari GuardDuty

Jenis: Penyebaran

Deskripsi: Aktifkan GuardDuty kemampuan Amazon yang dipilih untuk terus memantau, menganalisis, dan memproses sumber AWS data dan log di AWS lingkungan Anda.

Manajemen postur dari AWS Hub Keamanan CSPM

Jenis: Penyebaran

Deskripsi: Konfigurasi ini mengaktifkan standar dan kontrol Security Hub CSPM, yang mendeteksi kapan AWS akun dan sumber daya Anda menyimpang dari praktik terbaik keamanan.

Manajemen kerentanan dari Amazon Inspector

Jenis: Kebijakan

Deskripsi: Konfigurasi ini mengaktifkan kemampuan Amazon Inspector tertentu yang secara otomatis menemukan beban kerja, instans, gambar kontainer, dan sumber daya lainnya, serta memindainya untuk mencari kerentanan dan paparan jaringan.

Mengaktifkan konfigurasi dengan jenis kebijakan

Prosedur berikut menjelaskan cara membuat konfigurasi dengan jenis kebijakan untuk akun AWS Organisasi Anda. Untuk membuat kebijakan konfigurasi, Anda harus terlebih dahulu membuat kebijakan administrator yang didelegasikan di akun manajemen AWS organisasi. Untuk informasi tentang membuat kebijakan administrator yang didelegasikan di Hub Keamanan, lihat Membuat kebijakan administrator yang didelegasikan di Hub Keamanan.

Untuk membuat kebijakan yang mengaktifkan dan menonaktifkan akun anggota

1. Masuk menggunakan AWS akun Anda dengan kredensional administrator yang didelegasikan. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Konfigurasi.
3. Pilih item dengan jenis kebijakan atau kebijakan dan penerapan dari katalog Konfigurasi. Untuk mengkonfigurasi Hub Keamanan sepenuhnya, pilih Hub Keamanan (kemampuan penting dan tambahan).
4. Pada halaman Konfigurasi Hub Keamanan, di bagian Detail, masukkan nama dan deskripsi untuk kebijakan.

5. Di bagian Kemampuan keamanan, pilih salah satu dari yang berikut ini:

   - Aktifkan semua kemampuan - Mengaktifkan semua kemampuan penting Hub Keamanan, analisis ancaman, dan kemampuan tambahan.
   - Sesuaikan kemampuan — Pilih kemampuan dari bagian Manajemen keamanan, Analisis ancaman, dan manajemen kerentanan. Anda tidak dapat membatalkan pilihan kemampuan yang merupakan bagian dari paket esensial Hub Keamanan.

6. Di bagian Pemilihan akun, pilih salah satu opsi berikut:

   - Semua unit organisasi dan akun — Menerapkan konfigurasi ke seluruh organisasi Anda.
   - Unit dan akun organisasi tertentu — Gunakan bilah pencarian atau pohon struktur organisasi untuk memilih unit organisasi dan akun tempat kebijakan berlaku.
   - Tidak ada unit organisasi atau akun — Tidak menerapkan konfigurasi ke unit organisasi atau akun apa pun.

7. Di bagian Wilayah, pilih salah satu dari berikut ini:

   - Aktifkan semua Wilayah - Secara opsional memilih apakah akan secara otomatis mengaktifkan Wilayah baru.
   - Nonaktifkan semua Wilayah - Secara opsional memilih apakah akan secara otomatis menonaktifkan Wilayah baru.
   - Tentukan Wilayah — Pilih Wilayah mana yang akan diaktifkan dan dinonaktifkan.

8. (Opsional) Untuk pengaturan lanj utan, lihat Operator warisan di Panduan AWS Organizations Pengguna.
9. (Opsional) Untuk tag Sumber daya, tambahkan tag sebagai pasangan kunci-nilai untuk membantu Anda mengidentifikasi konfigurasi.
10. Pilih Berikutnya.
11. Tinjau perubahan Anda, lalu pilih Ter apkan.

    Status konfigurasi kebijakan Anda ditampilkan di bagian atas halaman Kebijakan. Setiap kemampuan memberikan status yang menunjukkan apakah berhasil dikonfigurasi atau mengalami kegagalan penerapan. Untuk kegagalan apa pun, pilih tautan kegagalan untuk melihat detail lebih lanjut. Untuk melihat kebijakan efektif di tingkat akun, tinjau tab Organisasi di halaman Konfigurasi.

Mengaktifkan konfigurasi dengan jenis penerapan

Prosedur berikut menjelaskan cara membuat konfigurasi dengan jenis penerapan untuk akun AWS Organisasi Anda.

Untuk membuat penerapan yang mengaktifkan akun anggota

1. Masuk menggunakan AWS akun Anda dengan kredensional administrator yang didelegasikan. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Konfigurasi.
3. Pilih item dengan jenis penerapan dari katalog Konfigurasi.
4. Di bagian Kemampuan keamanan, pilih kemampuan keamanan untuk diaktifkan.
5. Di bagian Pemilihan akun, pilih salah satu opsi berikut:
   - Semua unit organisasi dan akun — Menerapkan penerapan ke seluruh organisasi Anda.
   - Unit dan akun organisasi tertentu — Gunakan bilah pencarian atau pohon struktur organisasi untuk memilih unit organisasi dan akun tempat penerapan berlaku.
   - Tidak ada unit atau akun organisasi — Tidak menerapkan penerapan ke unit atau akun organisasi mana pun.
6. Di bagian Wilayah, pilih salah satu dari berikut ini:
   - Aktifkan semua Wilayah - Secara opsional memilih apakah akan secara otomatis mengaktifkan Wilayah baru.
   - Nonaktifkan semua Wilayah - Secara opsional memilih apakah akan secara otomatis menonaktifkan Wilayah baru.
   - Tentukan Wilayah — Pilih Wilayah mana yang akan diaktifkan dan dinonaktifkan.
7. Pilih Konfigurasikan

Mengedit kebijakan konfigurasi

Anda dapat mengedit kemampuan, Wilayah, dan akun yang terkait dengan kebijakan konfigurasi. Saat Anda membuka kebijakan untuk diedit, konsol menampilkan konfigurasi saat ini.

> **Note**
>
> Perubahan hanya berlaku untuk kemampuan yang Anda pilih dalam kebijakan yang diperbarui. Kemampuan yang tidak dipilih mempertahankan konfigurasi yang ada di seluruh akun dan Wilayah dalam kebijakan.

Untuk mengedit kebijakan konfigurasi

1. Masuk menggunakan AWS akun Anda dengan kredensional administrator yang didelegasikan. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Konfigurasi.
3. Di tab Kebijakan yang dikonfigurasi, pilih tombol radio untuk kebijakan yang ingin Anda edit, lalu pilih Edit.
4. Di bagian Kemampuan, pilih salah satu dari berikut ini:
   - Mengkonfigurasi dan mengaktifkan semua kemampuan — Mengaktifkan semua kemampuan dalam kebijakan.
   - Pilih kemampuan individual dan pilih Aktifkan, N onaktifkan, atau K ustom untuk masing-masing.
5. Di bagian Pemilihan akun, pilih salah satu opsi berikut:
   - Semua unit organisasi dan akun — Menerapkan kebijakan ke seluruh organisasi Anda.
   - Unit dan akun organisasi tertentu — Gunakan bilah pencarian atau pohon struktur organisasi untuk memilih unit organisasi dan akun tempat kebijakan berlaku.
   - Tidak ada unit organisasi atau akun — Menghapus kebijakan dari semua target.
6. Di bagian Wilayah, konfigurasikan Wilayah mana yang diterapkan kebijakan tersebut. Opsi tergantung pada pilihan Kemampuan Anda.

   Jika Anda memilih untuk mengaktifkan semua kemampuan:

   - Di semua kemampuan yang dipilih — Menetapkan konfigurasi Wilayah yang sama untuk semua kemampuan.
   - Per kemampuan - Memungkinkan Anda memilih Wilayah secara individual untuk setiap kemampuan.

Kemudian pilih Aktifkan semua Wilayah (dengan opsi untuk secara otomatis mengaktifkan Wilayah baru) atau Aktifkan di beberapa Wilayah untuk memilih Wilayah tertentu.

Jika Anda memilih tindakan campuran (mengaktifkan, menonaktifkan, atau kustom) untuk kemampuan individual:

- Jika semua kemampuan yang dipilih berbagi tindakan yang sama, pilih Di seluruh kemampuan yang dipilih untuk mengatur Wilayah secara seragam. Untuk mengatur Wilayah untuk setiap kemampuan secara individual, pilih Per kemampuan.
- Jika kemampuan memiliki tindakan yang berbeda, Anda harus menetapkan Wilayah untuk setiap kemampuan secara individual.
- Untuk kemampuan dengan tindakan K ustom, pilih Di seluruh kemampuan yang dipilih untuk mengatur Wilayah secara seragam untuk semua kemampuan. Untuk mengonfigurasi Wilayah untuk setiap kemampuan secara terpisah, pilih Per kemampuan.

7. Pilih Berikutnya.
8. Tinjau perubahan Anda, lalu pilih Per barui. Kebijakan yang diperbarui mengonfigurasi akun target.

Menghapus kebijakan konfigurasi

Anda dapat menghapus kebijakan konfigurasi. Saat Anda menghapus kebijakan, layanan akan menghapus semua akun terlampir dan unit organisasi dari kebijakan.

Untuk menghapus kebijakan konfigurasi

1. Masuk menggunakan AWS akun Anda dengan kredensional administrator yang didelegasikan. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Konfigurasi.
3. Di tab Kebijakan yang dikonfigurasi, pilih kebijakan yang ingin Anda hapus, lalu pilih H apus.
4. Masukkan `delete` di kotak konfirmasi, lalu pilih H apus.

Menghapus akun administrator yang didelegasikan di Hub Keamanan

Anda dapat menghapus akun administrator yang didelegasikan di konsol Hub Keamanan kapan saja. Namun, tindakan ini menghapus administrator yang didelegasikan dari Hub Keamanan dan CSPM

Hub Keamanan. Sebaiknya lakukan tindakan ini hanya jika Anda telah mengkonfirmasi operasi ini dengan akun keamanan Anda.

> **Note**
>
> Jika Anda menggunakan akun selain akun manajemen organisasi sebagai administrator yang didelegasikan CSPM Hub Keamanan, menghapusnya melalui konsol CSPM Security Hub atau AWS Organizations API juga menghapusnya dari Hub Keamanan.
> Demikian pula, jika Anda menghapus administrator yang didelegasikan Hub Keamanan melalui Konsol Hub Keamanan atau AWS Organizations API, itu juga dihapus dari Security Hub CSPM. Ketika administrator yang didelegasikan dihapus dari CSPM Hub Keamanan, Konfigurasi Pusat secara otomatis memilih keluar.

Untuk menghapus akun administrator yang didelegasikan

1. Masuk ke AWS akun Anda dengan kredensional akun manajemen organisasi Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Umum.
3. Di Administrator yang dideleg asikan, pilih H apus administrator yang didelegasikan. Di kotak dialog konfirmasi, masukkan hapus, dan pilih H apus.

Re-enabling Hub Keamanan

Sebelum mengaktifkan kembali Hub Keamanan pada akun yang sebelumnya dinonaktifkan menggunakan kebijakan Hub Keamanan, Anda harus melepaskan kebijakan penonaktifan terlebih dahulu. Jika Anda mencoba mengaktifkan kembali Hub Keamanan sementara kebijakan penonaktifan masih dilampirkan ke akun atau unit organisasi, kebijakan menonaktifkan akan mengesampingkan pengaktifan dan Hub Keamanan tetap dinonaktifkan.

Untuk menghapus kebijakan menonaktifkan Hub Keamanan untuk organisasi atau akun

1. Masuk menggunakan AWS akun Anda dengan kredensional akun manajemen organisasi Anda. Buka AWS Organizations konsol di https://console.aws.amazon.com/organizations/v2/home.
2. Dari panel navigasi pilih AWS akun.
3. Jika kebijakan penonaktifan Hub Keamanan saat ini adalah untuk seluruh organisasi Anda, pilih Root di bawah Struktur organisasi. Jika kebijakan penonaktifan Hub Keamanan saat ini adalah

untuk akun tertentu, pilih akun tertentu di bawah Struktur organisasi, lalu ikuti langkah-langkah yang tersisa untuk setiap akun.

4. Di tab Kebijakan, temukan bagian berjudul Kebijakan Hub Keamanan.
5. Pilih tombol radio di sebelah kebijakan yang menonaktifkan Hub Keamanan. Pilih Lepaskan.

Setelah melepaskan kebijakan dari organisasi atau akun, Anda dapat mengaktifkan kembali Hub Keamanan. Lihat Mengelola konfigurasi akun anggota di AWS Organisasi untuk detail tentang mengaktifkan kembali Hub Keamanan.

Rekomendasi Hub Keamanan

Layanan keamanan berikut AWS mengirimkan temuan ke Security Hub dalam format OCSF. Setelah Anda mengaktifkan Hub Keamanan, aktifkan ini Layanan AWS untuk keamanan tambahan.

Hub Keamanan CSPM

Saat Anda mengaktifkan Security Hub CSPM, Anda mendapatkan tampilan komprehensif tentang status keamanan Anda di. AWS Ini membantu Anda menilai lingkungan Anda terhadap standar industri keamanan dan praktik terbaik. Meskipun Anda dapat memulai dengan Security Hub tanpa mengaktifkan Security Hub CSPM, mengaktifkan Security Hub CSPM memungkinkan Security Hub untuk menghubungkan sinyal keamanan dari Security Hub CSPM untuk meningkatkan manajemen postur Anda.

Jika Anda mengaktifkan Security Hub CSPM, sebaiknya aktifkan standar Prakti k Terbaik AWS Keamanan Dasar untuk akun Anda. Standar ini terdiri dari serangkaian kontrol yang mendeteksi kapan Anda Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan. Saat Anda mengaktifkan standar AWS Praktik Terbaik Keamanan Dasar untuk akun Anda, AWS Security Hub CSPM secara otomatis mengaktifkan semua kontrolnya, termasuk kontrol untuk jenis sumber daya berikut:

- Kontrol akun
- Kontrol Amazon DynamoDB
- Kontrol Amazon Elastic Compute Cloud
- AWS Identity and Access Management (IAM) kontrol
- AWS Lambda kontrol
- Kontrol Layanan Database Relasional Amazon (Amazon RDS)

- Kontrol Layanan Penyimpanan Sederhana Amazon

Anda dapat menonaktifkan salah satu kontrol dalam daftar ini. Namun, jika Anda menonaktifkan salah satu kontrol ini, Anda tidak dapat menerima temuan eksposur untuk sumber daya yang didukung. Untuk informasi tentang kontrol yang berlaku untuk standar Praktik AWS Terbaik Keamanan Dasar, lihat Standar Praktik Terbaik AWS Keamanan Dasar v1.0.0 (FSBP).

GuardDuty

Saat Anda mengaktifkan GuardDuty, Anda dapat melihat semua temuan ancaman dan cakupan keamanan Anda di dasbor konsol Hub Keamanan. Jika Anda mengaktifkan GuardDuty, GuardDuty secara otomatis mulai mengirim data ke Hub Keamanan dalam format OCSF.

Amazon Inspector

Saat mengaktifkan Amazon Inspector, Anda dapat melihat semua temuan eksposur dan cakupan keamanan di dasbor konsol Security Hub. Jika Anda mengaktifkan Amazon Inspector, Amazon Inspector secara otomatis mulai mengirim data ke Hub Keamanan dalam format OCSF.

Sebaiknya aktifkan pemindaian Amazon EC2 dan pemindaian standar Lambda. Saat Anda mengaktifkan pemindaian Amazon EC2, Amazon Inspector memindai instans Amazon EC2 di akun Anda untuk mencari kerentanan paket dan masalah jangkauan jaringan. Saat Anda mengaktifkan pemindaian standar Lambda, Amazon Inspector memindai fungsi Lambda untuk mencari kerentanan perangkat lunak dalam dependensi paket. Untuk informasi selengkapnya, lihat Mengaktifkan jenis pemindaian di Panduan Pengguna Amazon Inspector.

Macie

Saat mengaktifkan Macie, Anda dapat mendeteksi eksposur tambahan untuk bucket Amazon S3 Anda. Sebaiknya konfigurasi penemuan data sensitif otomatis, sehingga Macie dapat mengevaluasi inventaris bucket Amazon S3 Anda setiap hari.

Cakupan akun di Security Hub

Halaman cakupan Akun menunjukkan akun dan Wilayah di organisasi Anda yang mengaktifkan Security Hub dan kemampuan keamanan terintegrasinya. Kemampuan ini termasuk layanan seperti Amazon Inspector, Amazon GuardDuty, AWS Security Hub CSPM, dan Amazon Macie. Gunakan halaman ini untuk mengidentifikasi kesenjangan cakupan dan melacak adopsi kemampuan di seluruh organisasi Anda.

Halaman cakupan akun

Dengan halaman cakupan akun, Anda dapat melihat metrik cakupan agregat. Gunakan tab Akun untuk detail tingkat akun dan tab Temuan Cakupan untuk meninjau kesenjangan cakupan tertentu.

Untuk mengakses Security Hub Cakupan akun halaman

1. Buka konsol Security Hub di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, di bawah Pengaturan pilih Cakupan akun.

Bagian ikhtisar

Bagian Ikhtisar menampilkan metrik cakupan keamanan gabungan di semua akun yang dipantau. Untuk akun administrator yang didelegasikan, bagian ini menampilkan detail pengaktifan Security Hub di seluruh organisasi, memberikan visibilitas ke cakupan untuk semua akun anggota. Visualisasi tingkat tinggi ini menunjukkan persentase akun dengan Security Hub dan setiap kemampuan keamanan yang diaktifkan, menawarkan pandangan komprehensif tentang postur keamanan Anda. Anda dapat memilih persentase cakupan Security Hub untuk melihat rincian akun yang diaktifkan menurut Wilayah. Anda dapat memilih setiap persentase kemampuan untuk memfilter temuan cakupan dengan kemampuan itu.

Persentase di bagian Ikhtisar ditentukan dengan menggunakan perhitungan berikut:

- Pengaktifan Security Hub = (Jumlah pasangan akun dan Wilayah tempat Security Hub diaktifkan) ÷ (Total akun di organisasi Anda × Wilayah tempat Security Hub tersedia)
- Cakupan layanan = (Jumlah akun yang diaktifkan dan pasangan Wilayah yang dikonfigurasi di mana kemampuan diaktifkan) ÷ (Jumlah total akun yang diaktifkan dan pasangan Wilayah yang dikonfigurasi, di Wilayah yang dikonfigurasi tempat akun diaktifkan, dan kemampuan tersedia)

> **Wilayah yang Dikonfigurasi**
>
> Untuk pengaturan Wilayah rumah, Wilayah yang dikonfigurasi menyertakan Wilayah asal dan Wilayah yang ditautkan. Untuk semua pengaturan lainnya, Wilayah yang dikonfigurasi hanya mengacu pada Wilayah saat ini.

Tab akun

Tab ini hanya tersedia di akun administrator yang didelegasikan Security Hub. Gunakan tab Akun untuk menganalisis cakupan khusus akun. Kolom Security Hub menunjukkan jumlah Wilayah tempat Security Hub diaktifkan untuk setiap akun. Kolom ini tidak ditampilkan saat melihat tab di Wilayah opt-in (Wilayah yang dinonaktifkan secara default). Setiap kemampuan keamanan menampilkan persentase cakupan yang, ketika dipilih, mengungkapkan rincian rinci fitur individual dan persentase cakupannya dalam kemampuan itu. Saat Anda memilih persentase ini, Security Hub memfilter hasilnya untuk menampilkan cakupan untuk kemampuan dan akun tersebut.

Persentase di tab Akun ditentukan menggunakan perhitungan berikut:

Cakupan tab Akun = (Jumlah Wilayah di mana kemampuan diaktifkan) ÷ (Wilayah di mana kemampuan tersedia)

Ada beberapa kasus di mana persentase cakupan mungkin ditampilkan sebagai 0%:

- Security Hub tidak diaktifkan di akun sehingga tidak ada temuan cakupan yang dicerna.
- Security Hub sedang menunggu temuan cakupan yang akan dihasilkan.

Tab temuan cakupan

Tab temuan Cakupan mencantumkan temuan informasi untuk kemampuan keamanan yang diaktifkan atau dinonaktifkan di seluruh akun dan Wilayah Anda. Temuan ini membantu mengidentifikasi area di mana cakupan keamanan dapat ditingkatkan. Setiap temuan menunjukkan judul temuan, akun dan Wilayah yang terpengaruh, dan status saat ini. Setiap temuan juga memiliki tautan konfigurasi yang membawa Anda ke layanan individual tempat Anda dapat mengelola konfigurasi untuk kemampuan itu, atau ke halaman konfigurasi Security Hub tempat Anda dapat memperbarui konfigurasi untuk layanan keamanan.

Anda dapat menekan temuan cakupan dengan status Tidak Tercakup jika kemampuan keamanan tersebut tidak berlaku untuk kombinasi Account-region. Security Hub mengecualikan temuan yang ditekan dari perhitungan persentase cakupan keamanan.

Untuk informasi lebih lanjut tentang temuan cakupan dan cara menekannya, lihat Temuan Cakupan di Security Hub.

Widget cakupan keamanan

Cakupan akun juga dapat dilihat melalui widget cakupan Keamanan di dasbor ringkasan Security Hub. Untuk informasi selengkapnya, lihat Widget cakupan keamanan.

Paket Diperpanjang Hub Keamanan

Dengan paket Security Hub Extended, Anda dapat melindungi seluruh properti perusahaan Anda di cloud, titik akhir, jaringan, identitas, data, email, dan browser. Gunakan AWS Security Hub sebagai pusat pengalaman operasi keamanan terintegrasi. Dengan paket Security Hub Extended, Anda dapat memilih solusi mitra yang memenuhi kebutuhan keamanan Anda dan mendaftar untuk harga bayar sesuai penggunaan yang fleksibel tanpa perlu investasi di muka atau komitmen jangka panjang. Anda dapat menambah atau menghapus solusi mitra saat kebutuhan bisnis Anda berkembang.

Paket Security Hub Extended tersedia untuk semua pelanggan yang telah mengaktifkan paket Security Hub Essentials. Biaya untuk paket Security Hub Extended muncul di AWS tagihan bulanan Anda dengan AWS sebagai penjual catatan.

Harga paket Extended Hub Security Hub untuk semua solusi tersedia di tab Paket Extended di halaman detail harga Hub Keamanan.

Izin untuk paket Security Hub Extended

Untuk berlangganan produk mitra dari paket Security Hub Extended, Anda memerlukan izin berikut, selain izin Hub Keamanan Anda:

- `aws-marketplace:ViewSubscriptions`
- `aws-marketplace:Subscribe`

Untuk berhenti berlangganan produk mitra dalam paket Security Hub Extended, Anda memerlukan izin berikut, selain izin Hub Keamanan Anda:

- `license-manager:ListReceivedLicenses`
- `aws-marketplace:ListAgreementCharges`
- `aws-marketplace:Unsubscribe`

Untuk informasi selengkapnya tentang izin AWS Marketplace, lihat Mengontrol akses ke langganan AWS Marketplace di Panduan AWS Pembeli Marketplace.

Meninjau dan mendaftar untuk mitra paket Extended

Paket Security Hub Extended dapat diakses melalui akun administrator yang didelegasikan Hub Keamanan atau akun mandiri. Di halaman paket Security Hub Extended, Anda dapat melihat detail tentang setiap mitra, memulai langganan solusi mitra, dan memulai proses orientasi ke setiap solusi mitra melalui halaman orientasi mitra.

Untuk mengakses paket Security Hub Extended dan mendaftar untuk produk mitra

1. Masuk ke Konsol AWS Manajemen menggunakan administrator yang didelegasikan atau kredentif akun mandiri.
2. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
3. Di panel navigasi, pilih Manajemen, lalu pilih Paket yang diperpanjang.
4. Untuk setiap solusi mitra yang ingin Anda daftarkan, pilih Lihat produk.
5. Tinjau detail harga produk, lalu pilih Ber langganan saat Anda siap memulai proses orientasi ke produk mitra.
6. Setelah proses berlangganan selesai, pilih Si apkan akun Anda untuk dialihkan ke halaman pendaftaran mitra.
7. Berikan informasi yang diperlukan untuk halaman pendaftaran mitra, dan ikuti langkah selanjutnya, yang disediakan oleh mitra, untuk menyelesaikan langkah orientasi.

> **Important**
>
> Anda tidak ditagih untuk solusi mitra sampai Anda menyelesaikan proses orientasi untuk produk mitra.

Berhenti berlangganan dari mitra paket Extended

Jika Anda tidak ingin lagi menggunakan solusi mitra paket Extended, Anda dapat berhenti berlangganan dari daftar mitra.

Untuk berhenti berlangganan dari solusi mitra, ikuti panduan di Mem batalkan langganan SaaS Anda di Panduan Pembeli AWS Marketplace.

> **Important**
>
> Selain membatalkan langganan Anda, ikuti langkah-langkah offboarding tambahan yang diperlukan untuk solusi mitra, berdasarkan cara Anda mengonfigurasi solusi untuk perusahaan Anda.

Memahami agregasi lintas wilayah di Hub Keamanan

Saat Anda mengaktifkan agregasi lintas wilayah di Hub Keamanan, Anda menetapkan Wilayah beranda. Wilayah asal mengumpulkan temuan, sumber daya, dan tren dari satu atau lebih Wilayah terkait. Anda kemudian dapat mengelola semua data keamanan dari satu Wilayah.

Misalkan Anda menetapkan AS Timur (Virginia Utara) sebagai Wilayah asal, dan AS Barat (Oregon) dan AS Barat (California Utara) sebagai Wilayah yang terhubung. Ketika Anda melihat halaman Temuan di AS Timur (Virginia Utara), Anda melihat temuan dari ketiga Wilayah. Pembaruan temuan tersebut juga tercermin di ketiga Wilayah.

Jenis data yang digabungkan

Ketika agregasi lintas wilayah diaktifkan dengan satu atau lebih Wilayah tertaut, Hub Keamanan mereplikasi data berikut dari Wilayah yang ditautkan ke Wilayah asal. Hal ini terjadi di setiap akun yang mengaktifkan agregasi lintas wilayah.

- Temuan
- Sumber daya
- Tren

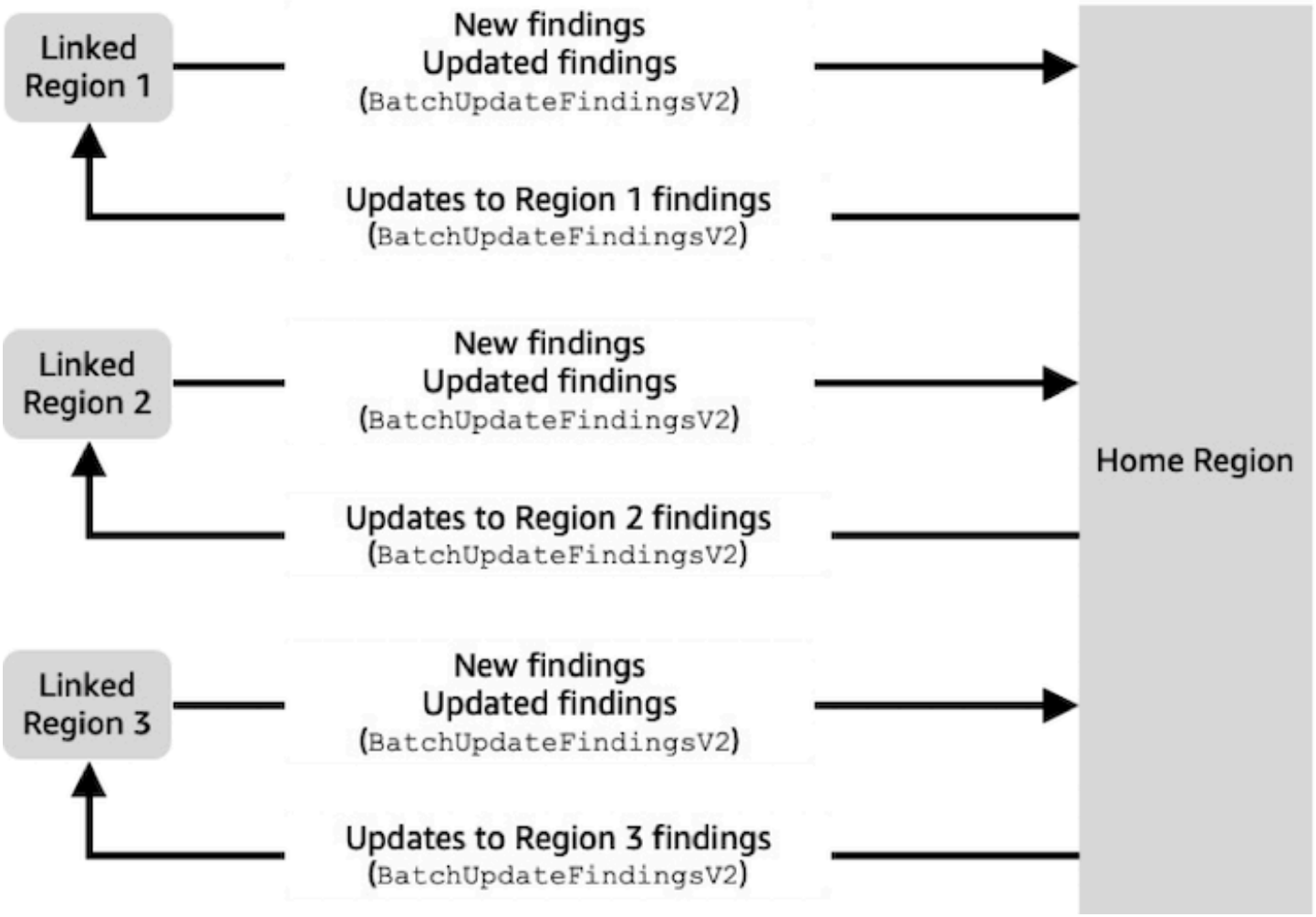
Selain data baru dalam daftar sebelumnya, Security Hub juga mereplikasi pembaruan data ini antara Wilayah yang ditautkan dan Wilayah asal. Pembaruan yang terjadi di Wilayah tertaut direplikasi ke Wilayah asal. Pembaruan yang terjadi di Wilayah beranda direplikasi kembali ke Wilayah yang ditautkan. Jika ada pembaruan yang saling bertentangan di Wilayah beranda dan Wilayah yang ditautkan, maka pembaruan terbaru digunakan.

Setiap temuan yang ada di suatu Wilayah pada saat itu menjadi Wilayah terkait tidak direplikasi ke Wilayah asal kecuali ada pembaruan pada temuan tersebut. Setelah Wilayah ditautkan ke Wilayah asal, ada perbedaan dalam temuan antara Wilayah asal dan Wilayah terkait sampai temuan di Wilayah terkait diperbarui atau mereka menua.

Setiap sumber daya yang ada di Wilayah pada saat menjadi Wilayah tertaut direplikasi ke Wilayah asal, biasanya dalam waktu 24-48 jam setelah Wilayah menjadi terhubung ke Wilayah asal.

Saat menghapus Wilayah yang ditautkan, temuan atau sumber daya apa pun untuk Wilayah tersebut tetap berada di Wilayah asal sampai temuan atau sumber daya habis.

Data tren didasarkan pada temuan dan sumber daya yang ada di Wilayah yang menjadi tujuan tren tersebut. Data tren di Wilayah asal mencerminkan keadaan temuan dan sumber daya saat ini yang telah disinkronkan ke Wilayah asal.



Cross-Region agregasi tidak menambah biaya Hub Keamanan. Anda tidak dikenakan biaya saat Hub Keamanan mereplikasi data atau pembaruan baru.

Di Wilayah beranda, halaman Ringkasan menyediakan tampilan temuan dan sumber daya aktif Anda di seluruh Wilayah yang ditautkan.

Security Hub hanya mengumpulkan data dari Wilayah di mana akun mengaktifkan Hub Keamanan. Hub Keamanan tidak diaktifkan secara otomatis untuk akun berdasarkan konfigurasi agregasi lintas wilayah.

Agregasi lintas wilayah dapat diaktifkan tanpa Daerah tertaut yang dipilih. Dalam hal ini, tidak ada replikasi data yang terjadi.

Agregasi untuk akun administrator dan anggota

Akun mandiri dan akun administrator dapat mengonfigurasi agregasi lintas wilayah. Jika dikonfigurasi oleh administrator, keberadaan akun administrator sangat penting agar agregasi lintas wilayah berfungsi di akun yang dikelola. Jika akun administrator dihapus atau dipisahkan dari akun anggota, agregasi lintas wilayah berhenti untuk akun anggota tersebut. Namun, jika akun anggota memiliki konfigurasi agregasi lintas wilayah sendiri sebelum dikaitkan dengan administrator, konfigurasi tersebut akan kembali berlaku.

Ketika akun administrator mengaktifkan agregasi lintas wilayah, Security Hub mereplikasi data yang dihasilkan akun administrator di semua Wilayah yang ditautkan ke Wilayah asal. Selain itu, Security Hub mengidentifikasi akun anggota yang terkait dengan administrator tersebut, dan setiap akun anggota mewarisi pengaturan agregasi lintas wilayah administrator. Security Hub mereplikasi data yang dihasilkan akun anggota di semua Wilayah yang ditautkan ke Wilayah asal.

Administrator dapat mengakses dan mengelola temuan keamanan dari semua akun anggota dalam Wilayah yang dikelola. Selain itu, administrator dapat melihat inventaris sumber daya dari semua akun anggota dalam Wilayah yang dikelola.

Sebagai akun anggota Hub Keamanan, Anda harus masuk ke Wilayah asal untuk melihat data agregat dari akun Anda dari semua Wilayah yang ditautkan. Akun anggota tidak memiliki izin untuk melihat data dari akun anggota lain dan tidak diizinkan untuk memanggil`CreateAggregatorV2`,`DeleteAggregatorV2`, dan `GetAggregatorV2` API.

Aturan otomatisasi dan agregasi lintas wilayah

Ketika agregasi lintas wilayah diaktifkan aturan otomatisasi hanya dapat dibuat di Wilayah beranda yang ditentukan. Aturan apa pun yang Anda tetapkan berlaku untuk semua Wilayah tertaut kecuali kriteria aturan Anda berlaku untuk wilayah tertentu. Anda harus membuat aturan otomatisasi terpisah untuk wilayah mana pun yang bukan Wilayah tertaut.

Aturan apa pun yang dibuat di Wilayah asal, sebelum mengaktifkan agregasi Lintas wilayah, secara otomatis berlaku di Wilayah yang ditautkan. Aturan yang sebelumnya dibuat di Wilayah tertaut tidak

akan lagi berlaku setelah agregator dibuat. Aturan yang ditentukan di Wilayah yang ditautkan kembali berlaku setelah agregator dihapus atau Wilayah tidak lagi ditautkan.

Mengaktifkan agregasi lintas wilayah

Anda harus mengaktifkan agregasi lintas wilayah dari Wil AWS ayah yang ingin Anda tentukan sebagai Wilayah asal.

Untuk mengaktifkan agregasi lintas wilayah, Anda membuat sumber daya Hub Keamanan yang disebut agregator pencarian. Sumber daya agregator pencarian menentukan Wilayah rumah Anda dan Wilayah tertaut (jika ada).

Anda tidak dapat menggunakan Wil AWS ayah yang dinonaktifkan secara default sebagai Wilayah rumah Anda. Untuk daftar Wilayah yang dinonaktifkan secara default, lihat Mengaktifkan Wilayah di Refer AWS ensi Umum.

Bila Anda mengaktifkan agregasi lintas wilayah, Anda memilih untuk menentukan satu atau lebih Wilayah tertaut jika diinginkan. Mengaktifkan agregasi lintas wilayah tidak mengaktifkan Hub Keamanan di Wilayah tersebut. Untuk mengaktifkan Hub Keamanan di wilayah, lihat Membuat kebijakan sebagai administrator yang didelegasikan untuk mengelola akun anggota di panduan pengguna Hub Keamanan.

Untuk mengaktifkan agregasi lintas wilayah (konsol)

1. Dari akun administrator atau di akun mandiri, buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/v2/home
2. Menggunakan pemilih Wil AWS ayah, masuk ke Wilayah yang ingin Anda gunakan sebagai Wilayah agregasi.
3. Di menu navigasi Hub Keamanan, pilih Peng aturan dan kemudian Umum.
4. Di bagian Cross-Region agregasi pilih Konfigurasi.
5. Secara default, Wilayah rumah disetel ke Tidak Ada Wilayah agregasi.
6. Di bawah Daer ah Beranda, pilih opsi untuk menetapkan Wilayah saat ini sebagai Wilayah rumah.
7. Secara opsional, untuk Wilayah Tertaut, pilih Wilayah untuk mengumpulkan data.
8. Pilih Simpan.

Meninjau pengaturan agregasi lintas wilayah

Anda dapat melihat konfigurasi agregasi lintas wilayah saat ini di Hub AWS Keamanan dari Wil AWS ayah mana pun di akun administrator atau di akun mandiri. Akun anggota tidak dapat melihat konfigurasi agregasi lintas wilayah. Konfigurasi mencakup Wilayah rumah, dan Wilayah yang ditautkan (jika ada).

Ikuti langkah-langkah untuk melihat setelan agregasi lintas wilayah Anda saat ini

Untuk melihat pengaturan agregasi lintas wilayah (konsol)

1. Buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Pada panel navigasi, pilih Peng aturan dan kemudian Umum.
3. Jika agregasi lintas wilayah tidak diaktifkan, maka halaman Umum menampilkan opsi untuk mengaktifkan agregasi lintas wilayah. Hanya akun administrator dan akun mandiri yang dapat mengaktifkan agregasi lintas wilayah.
4. Jika agregasi lintas wilayah diaktifkan, maka tab Wilayah menampilkan informasi berikut:
   - Wilayah asal
   - Apakah akan secara otomatis mengumpulkan temuan, sumber daya, dan tren dari Wilayah baru yang didukung Hub Keamanan dan yang Anda pilih
   - Daftar Wilayah tertaut (jika ada yang dipilih)

Memperbarui pengaturan agregasi lintas wilayah

Anda dapat memperbarui setelan agregasi lintas wilayah saat ini di Hub AWS Keamanan dengan mengubah Wilayah yang ditautkan atau Wilayah beranda saat ini.

Perubahan pada agregasi lintas wilayah tidak diterapkan untuk Wilayah pilihan hingga Anda mengaktifkan Wilayah di akun Anda. AWS Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 adalah Wilayah pilihan.

Saat Anda berhenti mengumpulkan data dari Wilayah tertaut, Hub AWS Keamanan tidak menghapus data agregat yang ada dari Wilayah tersebut yang dapat diakses di Wilayah asal.

Anda tidak dapat menggunakan prosedur pembaruan di bagian ini untuk mengubah Wilayah beranda. Untuk mengubah Wilayah rumah, Anda harus melakukan hal berikut:

1. Hapus konfigurasi agregasi lintas wilayah saat ini. Untuk petunjuk, lihat the section called “Menghapus agregasi”.
2. Ubah ke Wilayah yang Anda inginkan menjadi Wilayah rumah baru.
3. Aktifkan agregasi lintas wilayah. Untuk petunjuk, lihat the section called “Mengaktifkan agregasi”.

Anda harus memperbarui konfigurasi agregasi lintas wilayah dari Wilayah beranda saat ini.

Untuk mengubah Wilayah yang ditautkan (konsol)

1. Dari akun administrator atau di akun mandiri, buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Masuk ke Wilayah agregasi saat ini.
3. Di menu navigasi Hub Keamanan, pilih Peng aturan, lalu pilih Umum.
4. Untuk Cross-Region agregasi, pilih Edit.
5. Untuk Wil ayah Terta ut, perbarui Wilayah tertaut yang dipilih.
6. Pilih Simpan.

Menghapus agregasi lintas wilayah

Jika Anda tidak ingin AWS Security Hub mengumpulkan data, Anda dapat menghapus agregator temuan Anda. Atau, Anda dapat menyimpan agregator temuan Anda tetapi tidak menautkan Wil AWS ayah mana pun ke Wilayah asal dengan memperbarui agregator yang ada agar tidak ada Wilayah tertaut yang dipilih.

Untuk mengubah Wilayah rumah Anda, Anda harus menghapus agregator pencarian Anda saat ini dan membuat yang baru.

Saat Anda menghapus agregator temuan, Security Hub berhenti mengumpulkan data. Itu tidak menghapus data agregat yang ada dari Wilayah asal.

Menghapus agregator temuan (konsol)

Anda dapat menghapus agregator temuan Anda hanya dari Wilayah beranda saat ini.

Di Wilayah selain Wilayah rumah, panel agregasi Mencari pada konsol Hub Keamanan menampilkan pesan bahwa Anda harus mengedit konfigurasi di Wilayah beranda. Pilih pesan ini untuk menampilkan tautan untuk beralih ke Wilayah rumah.

Untuk menghentikan agregasi lintas wilayah (konsol)

1. Buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Pastikan Anda masuk ke Wilayah rumah Anda saat ini.
3. Di menu navigasi Hub Keamanan, pilih Peng aturan, lalu pilih Umum.
4. Di bawah Cross-Region agregasi, pilih Edit.
5. Di bawah Wilayah Agregasi, pilih Tanpa Wilayah agregasi.
6. Pilih Simpan.
7. Pada dialog konfirmasi, di bidang konfirmasi, ketik**`Confirm`**.
8. Pilih Konfirmasi.

Mengintegrasikan Hub Keamanan dengan Microsoft Azure

Untuk memantau sumber daya Microsoft Azure Anda, Anda dapat mengintegrasikan Microsoft Azure dengan Hub AWS Keamanan. Security Hub kemudian secara otomatis mengaktifkan manajemen postur dan manajemen kerentanan untuk lingkungan Azure Anda dan menghasilkan temuan dan data lain tentang lingkungan Anda. Anda tidak perlu mengaktifkan layanan keamanan Azure apa pun —semua fungsionalitas dilakukan oleh. AWS Lebih khusus lagi, layanan ini memberi Anda hal-hal berikut:

Benchmark Microsoft Azure Foundations CIS v4.0 dan Praktik Terbaik Dasar Azure

Pemeriksaan kepatuhan otomatis terhadap standar CIS Azure v4.0 dan standar Praktik Terbaik Dasar Azure. Standar ini mencakup identitas, jaringan, penyimpanan, logging, dan kontrol database.

Manajemen kerentanan

Amazon Inspector secara otomatis memindai gambar wadah Azure VM, Function Apps, dan Azure Container Registry (ACR) Anda untuk mencari kerentanan perangkat lunak melalui konektor tertaut layanan.

> **Note**
>
> Pemindaian VM memerlukan Amazon EC2 Systems Manager untuk dikonfigurasi di Wilayah yang sama. Untuk detail penyiapan, lihat dokumentasi Amazon Inspector untuk integrasi Azure.

Korelasi eksposur

Deteksi otomatis sumber daya Azure yang terekspos berdasarkan jangkauan jaringan, akses publik, dan kombinasi kesalahan konfigurasi.

Peringatan deteksi ancaman Microsoft Defender untuk Cloud

Jika Anda mengonfigurasi ekspor berkelanjutan Azure Defender ke Event Hub, Security Hub menyerap peringatan deteksi ancaman Defender for Cloud dan memetakannya ke format Open Cybersecurity Schema Framework (OCSF). Ini muncul di samping manajemen postur dan temuan kerentanan Anda di konsol Hub Keamanan.

Persediaan aset

Inventaris lengkap sumber daya Azure Anda yang ditemukan melalui integrasi, terlihat di konsol Hub Keamanan bersama AWS sumber daya Anda.

Format OCSF

Security Hub menghasilkan semua temuan dalam format Open Cybersecurity Schema Framework (OCSF), menyediakan skema yang konsisten di seluruh AWS dan temuan Azure.

Untuk membuat integrasi, Anda menghubungkan lingkungan Azure Anda ke Hub Keamanan melalui proses berikut:

1. Anda mengonfigurasi lingkungan Azure Anda dengan pendaftaran aplikasi, kredentif identitas federasi, penetapan peran Azure, dan infrastruktur Event Hub.
2. Dengan menggunakan konsol Hub Keamanan, Anda membuat konektor untuk integrasi. Anda menentukan ID penyewa Azure, ID klien aplikasi, cakupan pemantauan, dan wilayah Event Hub.
3. Security Hub menciptakan peran dan sumber daya terkait layanan yang diperlukan di Anda. Akun AWS
4. AWS Config mengumpulkan data konfigurasi sumber daya dari lingkungan Azure Anda.

   AWS Config digunakan secara internal untuk mengumpulkan data konfigurasi sumber daya. Tidak seperti manajemen AWS postur, di mana Anda harus secara eksplisit mengaktifkan AWS Config dan membayar untuk perekaman, manajemen postur Azure menangani AWS Config secara otomatis. Anda tidak perlu mengaktifkan AWS Config secara terpisah, mengkonfigurasi perekam, atau membayar secara terpisah untuk AWS Config penggunaan. Biaya ini sudah termasuk dalam harga Hub Keamanan Anda.

5. Security Hub mulai menerima data konfigurasi sumber daya dan peristiwa Log Aktivitas dari lingkungan Azure Anda.
6. Security Hub menghasilkan manajemen postur dan temuan kerentanan tentang lingkungan Azure Anda.

Bagaimana AWS Config digunakan

AWS Config digunakan secara internal untuk mengumpulkan data konfigurasi sumber daya dan mendeteksi perubahan di lingkungan Azure Anda. Konektor menangani ini secara otomatis. Anda tidak perlu mengaktifkan AWS Config secara terpisah, mengkonfigurasi perekam, atau membayar AWS Config penggunaan. Biaya ini termasuk dalam harga Hub Keamanan Anda untuk sumber daya Azure.

Informasi tambahan

Saat Anda membuat integrasi, Security Hub juga membuat integrasi terkait layanan terkait di Security Hub CSPM dan Amazon Inspector secara otomatis. Integrasi terkait layanan ini memastikan bahwa ruang lingkup pemeriksaan CSPM dan pemindaian kerentanan Inspektur sesuai dengan cakupan yang Anda tentukan di Hub Keamanan. Jika Anda ingin mengubah cakupan, Anda harus membuat perubahan di Hub Keamanan. Anda tidak dapat mengubah integrasi terkait layanan secara langsung di Security Hub CSPM atau Inspector.

Anda juga dapat membuat integrasi Azure secara langsung di Security Hub CSPM dan menentukan pengaturan lingkup independen. Integrasi CSPM kemudian beroperasi secara independen dari integrasi Hub Keamanan dan dapat memiliki cakupan Langganan Azure dan Wilayah Azure yang berbeda.

Untuk informasi tentang memperkirakan dan menghitung biaya untuk mengintegrasikan Hub Keamanan dengan Azure, lihat Harga Hub AWS Keamanan.

Topik

- Prasyarat untuk mengintegrasikan Hub Keamanan dengan Microsoft Azure
- Mengkonfigurasi Microsoft Azure untuk berintegrasi dengan Security Hub
- Mengkonfigurasi Hub Keamanan untuk berintegrasi dengan Microsoft Azure
- Menghapus konektor Microsoft Azure di Hub Keamanan

Prasyarat untuk mengintegrasikan Hub Keamanan dengan Microsoft Azure

Sebelum mengintegrasikan Microsoft Azure dengan AWS Security Hub, selesaikan tugas berikut di lingkungan Anda AWS dan Azure. Ini membantu memastikan bahwa Anda dan Security Hub memiliki sumber daya dan izin yang Anda butuhkan untuk memantau sumber daya Azure Anda.

Topik

- Prasyarat untuk AWS
- Prasyarat untuk Microsoft Azure

Prasyarat untuk AWS

Pastikan Anda memiliki hal-hal berikut di Akun AWS:

AWS Hub Keamanan diaktifkan

Hub Keamanan harus diaktifkan di Akun AWS dan Wilayah AWS di mana Anda ingin membuat konektor. Anda harus mengaktifkan Hub Keamanan sebelum membuat konektor Azure.

AWS Security Hub CSPM diaktifkan

Security Hub CSPM harus diaktifkan di dan. Akun AWS Wilayah AWS Integrasi Azure bergantung pada Security Hub CSPM untuk evaluasi konfigurasi sumber daya.

Izin IAM konsol

Prinsip IAM yang membuat konektor harus memiliki izin berikut:

- `config:GetConnector`
- `config:ListConnectors`
- `config:PutConnector`

Federasi Identitas Keluar IAM diaktifkan

Anda harus mengaktifkan Federasi Identitas Keluar IAM di. Akun AWS Fitur ini memungkinkan AWS layanan untuk mengotentikasi ke penyedia identitas eksternal (seperti Microsoft Entra ID) menggunakan kredenSIAL federasi daripada rahasia berumur panjang.

Setelah mengaktifkan Federasi Identitas Keluar, perhatikan URL Penerbit Token. URL ini mengikuti format:

```
https://uuid.tokens.sts.global.api.aws
```

Anda akan memerlukan URL ini saat mengonfigurasi kredentif identitas federasi di Azure.

Prasyarat untuk Microsoft Azure

Pastikan Anda memiliki hal-hal berikut di lingkungan Azure Anda:

Penyewa Azure

Anda harus memiliki penyewa Azure di cloud komersial Azure. Azure Government dan Azure China tidak didukung.

Ketersediaan log ID Microsoft Entra

Perekaman sumber daya memerlukan log audit Microsoft Graph dan log masuk dari penyewa ID Microsoft Entra Anda. Beberapa log ID Microsoft Entra memerlukan lisensi Microsoft Entra ID P1 atau P2.

Jika penyewa tidak memiliki log yang diperlukan, perekaman sumber daya mungkin melaporkan kegagalan sebagian. Pendaftaran aplikasi dan penetapan peran Azure tidak menyediakan data log yang hilang.

Peran Administrator Global

Anda harus memiliki peran Administrator Global di Microsoft Entra ID untuk mengonfigurasi lingkungan Azure. Peran ini diperlukan untuk mendaftarkan aplikasi, memberikan persetujuan admin untuk izin Microsoft Graph API, menetapkan peran RBAC di lingkup grup manajemen root penyewa, dan mengonfigurasi pengaturan diagnostik untuk Log Audit ID Entra.

Selain Administrator Global, Anda memerlukan peran Azure RBAC berikut untuk membuat sumber daya yang diperlukan integrasi:

- Administrator Akses Pengguna (atau Pemilik) di cakupan root (/) — untuk menetapkan peran RBAC di lingkup grup manajemen root penyewa.
- Kontributor Kebijakan Sumber Daya (atau Pemilik) di lingkup grup manajemen root penyewa — untuk membuat definisi dan penugasan Kebijakan Azure yang mengotomatiskan pengaturan diagnostik dan remediasi.
- Kontributor (atau Pemilik) di lingkup langganan yang menjadi tuan rumah Event Hub — untuk membuat namespace Event Hub dan sumber daya terkait.

> **Note**
>
> Di banyak organisasi, Azure Global Administrator dan administrator AWS keamanan adalah orang yang berbeda. Pengaturan Azure dapat diselesaikan secara independen menggunakan skrip pengaturan yang dihasilkan.

Setelah Anda menyelesaikan tugas-tugas ini, Anda siap untuk mengkonfigurasi lingkungan Azure Anda.

Mengkonfigurasi Microsoft Azure untuk berintegrasi dengan Security Hub

Setelah menyelesaikan tugas prasyarat, Anda dapat mengonfigurasi lingkungan Microsoft Azure Anda untuk mendukung integrasi dengan Hub AWS Keamanan. Untuk membantu Anda melakukan hal ini, konsol Hub Keamanan menghasilkan skrip penyiapan yang disesuaikan untuk konfigurasi Anda.

Untuk menghasilkan skrip penyiapan

1. Buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/advanced/home? wilayah = us-east-1. .
2. Di panel navigasi, pilih Integrasi.
3. Pilih Buat konektor Azure.
4. Lengkapi konfigurasi konektor (ID penyewa, ruang lingkup, dan nama), lalu salin skrip pengaturan yang dihasilkan.

Untuk menjalankan skrip, gunakan Azure CLI dan autentikasi dengan akun Administrator Global ()`az login`.

Ketika Anda menjalankan skrip, ia melakukan serangkaian tugas. Bagian berikut menjelaskan setiap tugas yang dilakukan skrip. Jika organisasi Anda membatasi eksekusi skrip, Anda dapat melakukan tugas ini secara manual, menggunakan topik ini sebagai panduan. Setelah mengonfigurasi lingkungan Azure Anda, Anda dapat mengonfigurasi Hub Keamanan untuk diintegrasikan dengan Azure.

Langkah 1—7 konfigurasikan fondasi bersama yang digunakan semua kemampuan Hub Keamanan: pendaftaran aplikasi, kredenSIAL federasi, penetapan peran Azure, izin Microsoft Graph, Event Hub,

dan ekspor log. Langkah 8—10 konfigurasikan sumber daya Azure tambahan untuk kemampuan tertentu:

- Manajemen kerentanan (Amazon Inspector) — Mengkonfigurasi ekspor peristiwa repositori Azure Container Registry (ACR) dan identitas terkelola yang ditetapkan sistem pada VM Azure Anda.
- Deteksi ancaman (Microsoft Defender for Cloud) — Mengkonfigurasi Microsoft Defender for Cloud untuk terus mengekspor peringatan keamanan ke Event Hub.

> **Note**
>
> Pendaftaran aplikasi Azure tunggal dibagikan di seluruh layanan AWS keamanan. Jika Anda juga menggunakan Security Hub CSPM atau Amazon Inspector untuk Azure, mereka menggunakan pendaftaran aplikasi yang sama. Anda tidak perlu membuat pendaftaran terpisah untuk setiap AWS layanan.

Tugas

- Langkah 1: Daftarkan aplikasi Azure
- Langkah 2: Buat prinsipal layanan
- Langkah 3: Konfigurasikan kredentif identitas federasi
- Langkah 4: Tetapkan peran RBAC
- Langkah 5: Konfigurasikan izin Microsoft Graph API
- Langkah 6: Siapkan Azure Event Hub
- Langkah 7: Konfigurasikan Log Aktivitas dan ekspor Log Audit ID Entra
- Langkah 8: Konfigurasikan ekspor Azure Container Registry
- Langkah 9: Aktifkan identitas terkelola di Azure VM
- Langkah 10: Ekspor Microsoft Defender untuk peringatan Cloud

Langkah 1: Daftarkan aplikasi Azure

Daftarkan aplikasi baru di Microsoft Entra ID. Aplikasi ini berfungsi sebagai identitas yang digunakan untuk men AWS gotentikasi ke lingkungan Azure Anda menggunakan kredenSIAL federasi. Tidak ada rahasia klien yang diperlukan.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Perhatikan ID Aplikasi (klien) dari output (`appId`atribut). Anda akan memberikan nilai ini saat membuat konektor di konsol Hub Keamanan.

Langkah 2: Buat prinsipal layanan

Buat prinsip layanan untuk aplikasi terdaftar. Anda menggunakan penetapan peran Azure untuk memberikan izin kepada prinsipal layanan. Prinsip layanan melakukan tindakan di lingkungan Azure Anda.

```
$ az ad sp create --id application-client-id
```

Di *`application-client-id`* mana ID Aplikasi (klien) dari langkah sebelumnya.

Setel URI ID Aplikasi pada pendaftaran ke`api://`*`application-client-id`*. AWS membutuhkan pengenal ini untuk bertukar token federasi dengan aplikasi. Tanpa URI ini, AWS tidak dapat menghasilkan audiens token federasi yang valid, dan setiap kemampuan gagal untuk mengotentikasi ke Azure.

```
$ az ad app update \
  --id application-client-id \
  --identifier-uris "api://application-client-id"
```

Langkah 3: Konfigurasikan kredentif identitas federasi

Konfigurasikan kredentif identitas federasi pada aplikasi AWS untuk memungkinkan otentikasi tanpa rahasia klien. Ini menetapkan kepercayaan OIDC antara AWS dan Azure. Tidak ada rahasia atau kredenSIAL berumur panjang yang disimpan.

Integrasi Azure Hub Keamanan mengautentikasi menggunakan satu peran AWS IAM per kemampuan: penemuan konfigurasi sumber daya, manajemen kerentanan, dan deteksi ancaman. Tambahkan kredensi identitas federasi untuk setiap peran sehingga setiap kemampuan dapat mengotentikasi ke Azure. AWS membuat peran terkait layanan secara otomatis saat Anda membuat konektor. Per `Inspector2SSMFederationRole` an yang digunakan untuk pemindaian VM bukanlah peran terkait layanan; Anda membuatnya sebagai bagian dari pengaturan pemindaian VM Amazon Inspector, yang dijelaskan pada Langkah 9.

Kemampuan	Subjek (peran IAM ARN)
Penemuan konfigurasi sumber daya (AWS Config)	`arn:aws:iam:: account-id :role/aws-service-role/thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty`
Manajemen kerentanan (Inspektur)	`arn:aws:iam:: account-id :role/aws-service-role/thirdparty.inspector2.amazonaws.com/AWSServiceRoleForAmazonInspector2ThirdParty`
Manajemen kerentanan - Pemindaian VM (Amazon EC2 Systems Manager)	`arn:aws:iam:: account-id :role/Inspector2SSMFederationRole- tenant-id`
Deteksi ancaman (Hub Keamanan)	`arn:aws:iam:: account-id :role/aws-service-role/securityhubv2.amazonaws.com/AWSServiceRoleForSecurityHubV2`

Jalankan perintah berikut sekali untuk setiap subjek di tabel sebelumnya, mengubah `subject` nilai `name` dan setiap kali. `audiences`Nilai `issuer` dan sama untuk setiap kredensi.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "credential-name",
    "issuer": "token-issuer-url",
    "subject": "service-linked-role-arn",
    "audiences": ["api://AzureADTokenExchange"],
    "description": "AWS federation for Security Hub Azure integration"
  }'
```

Nilai-nilai kunci:

- Penerbit — URL Penerbit Token Anda dari Federasi Identitas Keluar IAM. Ini mengikuti format`https://uuid.tokens.sts.global.api.aws`.
- Sub jek — Peran IAM ARN dari tabel sebelumnya. Per *tenant-id* an dalam Amazon EC2 Systems Manager adalah ID penyewa Azure Anda.

- Audiens — `api://AzureADTokenExchange` (nilai standar untuk federasi identitas beban kerja).
- Nama — Nama apa pun yang unik dalam aplikasi.

Langkah 4: Tetapkan peran RBAC

Tetapkan peran bawaan berikut ke prinsipal layanan:

- Pemb aca — Memberikan akses baca-saja ke semua sumber daya Azure, sehingga Hub Keamanan dapat menemukan dan mengevaluasi konfigurasi sumber daya Anda. Tetapkan peran ini di root scope (`/`).
- Kontributor — Memberikan akses tulis yang dibutuhkan Amazon Inspector untuk memindai mesin virtual Azure Anda, Aplikasi Fungsi, dan gambar wadah untuk mencari kerentanan. Tetapkan peran ini di lingkup grup manajemen root penyewa, yang menyebarkannya ke setiap langganan di penyewa.
- Penerima Data Azure Event Hubs - Memungkinkan AWS untuk membaca acara dari Event Hub. Tetapkan peran ini di lingkup grup manajemen root penyewa.

⚠ Tetapkan Pembaca di cakupan root

Pastikan untuk menetapkan peran Pembaca di cakupan root (`/`), bukan lingkup grup manajemen root penyewa. Security Hub membaca sumber daya penetapan peran Azure di setiap lingkup, termasuk penugasan yang dicakup di root penyewa. Penugasan Pembaca di grup manajemen root tidak mencakup penugasan yang cakupannya`/`, jadi tanpanya pembacaan tersebut gagal dengan kesalahan otorisasi dan konektor dapat memasuki keadaan terdegradasi.

⚠ Kontributor memberikan akses tulis di seluruh penyewa

Peran Kontributor di lingkup grup manajemen root penyewa memberikan akses penulisan di seluruh penyewa yang sangat istimewa ke sumber daya Azure Anda. Security Hub memerlukan akses ini agar Amazon Inspector dapat memindai sumber daya komputasi Anda untuk mencari kerentanan. Misalnya, Inspector menggunakan izin menjalankan perintah mesin virtual yang disediakan oleh Kontributor. Melalui Amazon EC2 Systems Manager

Automation, Inspector menjalankan perintah pada VM Azure Anda untuk menginstal dan mengoperasikan agen VM Scanner.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Contributor" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope "/providers/Microsoft.Management/managementGroups/tenant-id"

$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

Root-scope penugasan membutuhkan akses yang lebih tinggi

Menetapkan peran di cakupan root (/) memerlukan akses yang ditingkatkan. Jika penetapan peran gagal, verifikasi bahwa manajemen akses untuk sumber daya Azure disetel ke Ya di Microsoft Entra ID > Properti. Kemudian keluar dan masuk kembali untuk menyegarkan token Anda.

Hapus elevasi akar sementara

Meng aktifkan manajemen Akses untuk sumber daya Azure memberikan administrator yang masuk peran Administrator Akses Pengguna di cakupan root (/), yang dapat mengelola akses di setiap grup langganan dan manajemen di penyewa. Setelah orientasi selesai, setel Manajemen akses untuk sumber daya Azure kembali ke Tidak di Microsoft Entra ID > Properti, simpan, dan keluar sehingga elevasi ini tidak tetap aktif.

Langkah 5: Konfigurasikan izin Microsoft Graph API

Berikan izin Microsoft Graph API berikut (jenis Aplikasi) ke aplikasi, lalu berikan persetujuan admin:

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`
- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Langkah 6: Siapkan Azure Event Hub

AWS Config menggunakan Azure Event Hub untuk menerima pemberitahuan hampir real-time tentang perubahan konfigurasi sumber daya di lingkungan Azure Anda. Skrip penyiapan membuat infrastruktur Event Hub dan menandainya untuk penemuan. Penemuan Event Hub menggunakan resolusi berbasis tag: Security Hub mencari tag pada namespace Event Hub dengan format `AWSConfig-`*`account-id`*`-`*`region`* untuk mengidentifikasi instance Event Hub yang benar untuk integrasi Anda.

```
$ az group create \
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
```

```
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Setelah membuat Event Hub, beri tag namespace untuk penemuan dan tetapkan peran Penerima Data. Gunakan `az tag update` dengan `--operation merge` agar Anda mempertahankan tag lain di namespace (seperti tag penemuan deteksi ancaman dari Langkah 10):

```
$ az tag update \
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> Dalam format tag`AWSConfig-account-id-region`, *`account-id`* adalah Akun AWS ID 12 digit Anda dan *`region`* merupakan Wilayah AWS tempat Anda membuat konektor (misalnya,`us-east-1`). Nilai-nilai ini mengidentifikasi mana Akun AWS dan Wilayah yang memiliki integrasi Event Hub ini.

Konfigurasi kunci:

- Namespace SKU — Standar (diperlukan untuk kelompok konsumen).
- Nama Hub Acara `-activitylog`.
- Kelompok konsumen `-AWSConfig`.
- Tag - `AWSConfig-account-id-region` dengan nilai`activitylog`. Tag ini memungkinkan AWS Config untuk menemukan Event Hub secara otomatis.

- Penetapan peran — Penerima Data Hub Peristiwa Azure pada namespace.

Untuk deteksi ancaman, penyiapan juga membuat `defender-alerts` Event Hub terpisah dengan grup `AWSSecurityHub` konsumen, dan menambahkan tag penemuan kedua dalam format yang mengidentifikasi hub `AWSSecurityHub-account-id-region` yang dibaca Hub Keamanan secara langsung. Untuk informasi selengkapnya, lihat Langkah 10.

Langkah 7: Konfigurasikan Log Aktivitas dan ekspor Log Audit ID Entra

Konfigurasikan Azure untuk mengekspor Log Aktivitas dan log ID Microsoft Entra ke Event Hub.

Ekspor Log Aktivitas:

Konfigurasikan pengaturan diagnostik pada setiap langganan untuk mengekspor Log Aktivitas ke Hub Peristiwa. Skrip penyiapan mengonfigurasi ini secara otomatis untuk semua langganan yang dipantau. Log Aktivitas menangkap aktivitas tingkat langganan termasuk penetapan peran dan perubahan sumber daya.

Ekspor log ID Microsoft Entra:

Konfigurasikan pengaturan diagnostik pada Microsoft Entra ID untuk mengekspor log ke Event Hub yang sama. Arahkan ke Microsoft Entra ID > Pemantauan > Pengaturan diagnostik > Tambahkan pengaturan diagnostik. Akti AuditLogs fkan SignInLogs,, dan NonInteractiveUserSignInLogs, dan mengarahkannya ke Event Hub Anda.

Langkah 8: Konfigurasikan ekspor Azure Container Registry

Security Hub memindai gambar wadah Azure Container Registry (ACR) Anda untuk mencari kerentanan melalui Amazon Inspector. Untuk melakukan ini, Inspector memerlukan peristiwa repositori ACR yang diekspor ke Event Hub di wilayah Azure yang sama dengan registri. Untuk pengaturan ekspor ACR, lihat Mengon figurasi Amazon Inspector untuk mengintegrasikan dengan Microsoft Azure di Panduan Pengguna Amazon Inspector.

Langkah 9: Aktifkan identitas terkelola di Azure VM

Security Hub memindai mesin virtual Azure Anda melalui Inspector. Setiap VM Azure target harus mengaktifkan identitas terkelola yang ditetapkan sistem. Untuk menambahkan identitas ini ke VM Anda secara otomatis, tetapkan dua Kebijakan Azure yang menggunakan `modify` efek pada lingkup grup manajemen root penyewa:

- Untuk VM yang tidak memiliki identitas, kebijakan menambahkan identitas terkelola yang ditetapkan sistem.
- Untuk VM yang hanya memiliki identitas yang ditetapkan pengguna, kebijakan menambahkan identitas terkelola yang ditetapkan sistem sambil mempertahankan identitas yang ditetapkan pengguna yang ada.

VM yang sudah memiliki identitas terkelola yang ditetapkan sistem dibiarkan tidak berubah. Karena kebijakan menggunakan `modify` efek, mereka menyesuaikan identitas di tempat tanpa menyebarkan ulang VM.

Inspector menggunakan Amazon EC2 Systems Manager Automation untuk menyebarkan dan mengelola agen Inspector VM Scanner pada VM Azure Anda. Ini memerlukan pengaturan AWS sisi tambahan, termasuk penyedia identitas IAM OIDC untuk Microsoft Entra ID dan beberapa peran IAM. Untuk pengaturan pemindaian VM lengkap, lihat Mengon figurasi Amazon Inspector untuk mengintegrasikan dengan Microsoft Azure di Panduan Pengguna Amazon Inspector.

Langkah 10: Ekspor Microsoft Defender untuk peringatan Cloud

Security Hub menyerap peringatan deteksi ancaman Microsoft Defender for Cloud dan memetakannya ke format Open Cybersecurity Schema Framework (OCSF). Untuk mengirimkan peringatan ini, buat `defender-alerts` Event Hub khusus dan konfigurasikan Microsoft Defender for Cloud untuk terus mengekspor peringatan keamanan ke sana.

Di namespace Event Hub dari Langkah 6, buat `defender-alerts` Event Hub, grup `AWSSecurityHub` konsumen untuk dibaca Hub Keamanan, dan aturan otorisasi tanda tangan akses bersama (SAS) dengan cakupan hub dengan izin Kirim yang digunakan Microsoft Defender for Cloud untuk mengirim peringatan:

```
$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "defender-alerts" \
  --message-retention 3 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "AWSSecurityHub"
```

```
$ az eventhubs eventhub authorization-rule create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "defender-alerts" \
  --name "DefenderExportSend" \
  --rights Send
```

Kemudian, gabungkan tag penemuan kedua ke namespace sehingga Security Hub menemukan `defender-alerts` hub. Gunakan `az tag update` dengan `--operation merge` agar Anda mempertahankan tag `AWSConfig` penemuan dari Langkah 6:

```
$ az tag update \
  --resource-id namespace-resource-id \
  --operation merge \
  --tags "AWSSecurityHub-account-id-region=defender-alerts"
```

Terakhir, konfigurasikan Microsoft Defender untuk Cloud ekspor berkelanjutan dari tipe data peringatan keamanan ke `defender-alerts` Event Hub. Di portal Azure, buka Microsoft Defender for Cloud > Environment settings, pilih langganan, pilih Continuous export > Event Hub, pilih Security Alerts, dan pilih `defender-alerts` Event Hub dan aturan `DefenderExportSend` SAS.

> **Note**
>
> Jika Anda mengonfigurasi ekspor berkelanjutan secara terprogram (melalui Azure Resource Manager API, template ARM, atau Kebijakan Azure) daripada di portal, autentikasi ekspor ke Event Hub dengan string koneksi `DefenderExportSend` SAS. Ambil dengan `az eventhubs eventhub authorization-rule keys list` untuk `DefenderExportSend` aturan, dan tetapkan sebagai string koneksi tindakan ekspor. Untuk informasi selengkapnya, lihat Meng atur ekspor berkelanjutan di dokumentasi Microsoft Azure.

> **Note**
>
> Setelah Anda menyelesaikan tugas ini, tunggu sekitar 15-30 menit agar konfigurasi berlaku. Kemudian, verifikasi bahwa Event Hub Anda menerima pesan (IncomingMessagesmetrik) sebelum Anda membuat konektor di Hub Keamanan.

Mengkonfigurasi Hub Keamanan untuk berintegrasi dengan Microsoft Azure

Setelah menyelesaikan tugas prasyarat dan mengonfigurasi lingkungan Microsoft Azure Anda, Anda dapat mengonfigurasi Hub AWS Keamanan untuk diintegrasikan dengan Azure. Untuk mengkonfigurasi Hub Keamanan agar terintegrasi dengan Azure, Anda membuat konektor. Anda dapat membuat konektor dari akun Administrator Delegasi atau akun manajemen. Setelah Anda membuat konektor, peristiwa berikut terjadi:

1. Security Hub memvalidasi kredenSIAL Azure dan konektivitas ke lingkungan Azure Anda. Proses ini dapat memakan waktu beberapa menit.
2. Security Hub membuat konektor terkait layanan di Security Hub CSPM dan Amazon Inspector. Konektor ini memastikan bahwa pemeriksaan manajemen postur dan pemindaian kerentanan sesuai dengan cakupan yang Anda tentukan di Hub Keamanan.
3. AWS Config mulai menemukan sumber daya Azure menggunakan kredentif identitas federasi.
4. Security Hub secara otomatis mengaktifkan standar CIS Microsoft Azure Foundations Benchmark v4.0 dan standar Praktik Terbaik Azure Foundational di CSPM untuk sumber daya Azure Anda.
5. Temuan awal mulai muncul dalam waktu 15—30 menit untuk sumber daya dengan peristiwa Log Aktivitas. Evaluasi penuh dari semua sumber daya yang ada dapat memakan waktu hingga 24 jam.

Topik

- Buat konektor Azure
- Sesuaikan ruang lingkup konektor Azure
- Verifikasi kesehatan konektor Azure
- Memecahkan masalah konektor Azure
- Bagaimana Security Hub menangani sumber daya dan menemukan pengidentifikasi

Buat konektor Azure

Untuk membuat konektor Microsoft Azure untuk lingkungan Anda, selesaikan langkah-langkah berikut dengan menggunakan konsol Hub AWS Keamanan atau API.

1. Buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/advanced/home? wilayah = us-east-1. .
2. Di panel navigasi, pilih Integrasi.

3. Pilih Buat konektor Azure.
4. Di bagian Kemampuan keamanan, pilih apakah Anda ingin fitur pemindaian jaringan diaktifkan. Fitur ini diaktifkan secara default untuk akun tempat Anda mengaktifkan integrasi Azure, dan dapat dihapus centang sebelum menyelesaikan penyiapan konektor Anda. Jika kebijakan organisasi memblokir fitur ini untuk akun Anda, fitur tersebut tidak muncul sebagai opsi. Untuk informasi selengkapnya, lihat Pemindaian jaringan di Hub Keamanan.
5. Untuk ID Penyewa Azure, masukkan pengenal penyewa Microsoft Entra ID Anda. Anda dapat menemukan ini di portal Azure di bawah Microsoft Entra ID > Properties > Tenant ID.
6. Untuk ID Aplikasi (klien), masukkan ID aplikasi untuk aplikasi Azure yang Anda daftarkan selama pengaturan lingkungan Azure.
7. Konfigurasikan pengaturan tambahan dan ruang lingkup konektor dengan melakukan hal berikut:

   - Untuk Nama, masukkan nama unik untuk konektor. Nama dapat berisi hingga 50 karakter alfanumerik dan dapat mencakup tanda hubung.

     > **Note**
     >
     > Nama konektor tidak dapat diubah setelah pembuatan.

   - Untuk Deskripsi, secara opsional masukkan deskripsi singkat konektor. Deskripsi dapat berisi hingga 200 karakter.

     > **Important**
     >
     > Nama dan deskripsi digunakan untuk mengidentifikasi konten Anda. Jangan menyertakan informasi sensitif, rahasia, atau identitas pribadi (PII) di dalamnya.

   - Untuk Langganan, pilih Semua langganan untuk memantau semua langganan saat ini dan yang akan datang di penyewa, atau Langganan khusus untuk memantau hanya langganan yang Anda tentukan. Jika Anda memilih untuk memantau hanya langganan tertentu, masukkan ID untuk masing-masing langganan.
   - Untuk Wil ayah, pilih Semua wilayah untuk memantau sumber daya di semua wilayah Azure, atau Wilayah tertentu untuk memantau hanya Wilayah yang Anda tentukan.

> **Note**
>
> Jika Anda sudah membuat konektor di Security Hub CSPM atau Amazon Inspector untuk penyewa Azure yang sama, cakupan konektor di Hub Keamanan harus menyertakan langganan dan Wilayah yang sama dengan konektor di Security Hub CSPM atau Amazon Inspector.

> **Note**
>
> Kontrol yang mengevaluasi sumber daya Microsoft Entra ID dan Microsoft Graph memerlukan cakupan Wilayah global untuk disertakan dalam konfigurasi integrasi Anda. Jika Anda memilih Wilayah Azure tertentu saja, kontrol ini tidak menghasilkan temuan.

8. Tinjau konfigurasi konektor.

> **Note**
>
> Jika Anda berencana menggunakan Amazon Inspector untuk pemindaian VM Azure, Anda harus membuat peran IAM yang diperlukan. Lihat perinciannya di the section called “Peran IAM untuk pemindaian VM”.

9. Setelah selesai memasukkan dan meninjau pengaturan, pilih Buat konektor.

Peran IAM untuk pemindaian VM Azure melalui Amazon Inspector

Untuk mengaktifkan pemindaian kerentanan melalui Amazon Inspector, Anda harus membuat sumber daya IAM berikut di. Akun AWS

Penyedia identitas IAM OIDC

Buat penyedia identitas IAM OIDC untuk Microsoft Entra ID dengan konfigurasi berikut:

- URL penerbit: `https://sts.windows.net/`*`tenant-id`*`/`
- Daftar ID klien: `api://`*`app-id`*, `api://AzureADTokenExchange`

- Sidik jari: String 40 karakter dari semua nol (`0`diulang 40 kali). AWS STS memvalidasi token melalui titik akhir JWKS daripada nilai sidik jari.

Inspector2VmScannerRole-*tenant-id*

Digunakan oleh agen Amazon Inspector VM Scanner yang berjalan di Azure VM untuk mengirim telemetri pemindaian ke Amazon Inspector. Peran ini menggunakan federasi identitas web OIDC melalui penyedia Microsoft Entra ID identitas.

Kebijakan kepercayaan:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::account-id:oidc-provider/
sts.windows.net/tenant-id/"
            },
            "Action": "sts:AssumeRoleWithWebIdentity"
        }
    ]
}
```

Tag:

- `inspector-managed` = `true`

Kebijakan izin (TelemetryPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2-telemetry:*",
            "Resource": "*"
        }
    ]
}
```

Inspector2SSMFederationRole-*tenant-id*

Mengaktifkan federasi OIDC ke Azure untuk otentikasi lintas cloud yang aman. Peran ini diasumsikan oleh AssumeRole dan DispatchRole, dan oleh Amazon EC2 Systems Manager, untuk mendapatkan token identitas web untuk operasi Azure.

Kebijakan kepercayaan:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalTag/caller": "SSM"
                },
                "ArnLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
                        "arn:aws:iam::account-id:role/Inspector2SSMDispatchRole-tenant-
id"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Kebijakan izin (FederationPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "sts:IdentityTokenAudience": [
                        "api://AzureADTokenExchange"
                    ]
                }
            },
            "Action": [
                "sts:GetWebIdentityToken",
                "sts:TagGetWebIdentityToken"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Tag:

- `caller` = `SSM`
- `inspector-managed` = `true`

Inspector2SSMAssumeRole-*tenant-id*

Mengeksekusi Otomatisasi Manajer Sistem Amazon EC2 untuk mengintegrasikan VM Azure sebagai instans terkelola. Peran ini membuat dan mengelola aktivasi hibrida, meneruskan peran ke Amazon EC2 Systems Manager, dan mengambil dokumen otomatisasi.

Kebijakan kepercayaan:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
```

```
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Kebijakan izin (AssumeRolePolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/
AmazonEC2RunCommandRoleForManagedInstances",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateActivation",
                "ssm:DeleteActivation",
                "ssm:DescribeActivations",
                "ssm:DescribeInstanceInformation",
                "ssm:PutConfigurePackageResult",
                "iam:ListRoleTags"
            ],
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ssm:AddTagsToResource",
            "Resource": [
                "arn:aws:ssm:*:account-id:activation/*",
                "arn:aws:ssm:*:account-id:managed-instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ssm:GetDocument",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:*:document/AWS-InstallSsmAgentOnAzure",
                "arn:aws:ssm:*::document/AmazonInspector2-InspectorVmScanner"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ssm:GetCloudConnector",
            "Resource": "*"
        }
    ]
}
```

Tag:

- `caller` = `SSM`
- `AzureTenantId` = *`tenant-id`*
- `AzureApplicationId` = *`app-id`*
- `inspector-managed` = `true`

Inspector2SSMDispatchRole-***`tenant-id`***

Menyelesaikan target VM Azure dan mengirimkan instalasi agen Amazon Inspector VM Scanner melalui Amazon EC2 Systems Manager Automation. Peran ini memulai eksekusi otomatisasi dan meneruskannya AssumeRole ke Amazon EC2 Systems Manager.

Kebijakan kepercayaan:

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id"
                }
            }
        }
    ]
}
```

Kebijakan izin (DispatchPolicy):

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/Inspector2SSMAssumeRole-tenant-
id",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ssm.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ssm:StartAutomationExecution",
            "Resource": [
                "arn:aws:ssm:*:*:document/AWS-InstallDistributorPackageOnAzure",
                "arn:aws:ssm:*:account-id:automation-execution/*"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::account-id:role/
Inspector2SSMFederationRole-tenant-id"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceInformation",
                "ssm:ListCloudConnectors",
                "ssm:GetCloudConnector",
                "iam:ListRoleTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Tag:

- `caller` = `SSM`
- `inspector-managed` = `true`

Prasyarat untuk pemindaian VM

Pendaftaran aplikasi Azure harus memiliki URI ID Aplikasi yang disetel ke`api://app-id`.

Setiap VM Azure yang ingin Anda pindai harus mengaktifkan identitas terkelola yang ditetapkan sistem. Untuk menetapkan identitas terkelola secara otomatis ke VM baru, gunakan DeployIfNotExists kebijakan di lingkungan Azure Anda.

Setelah Anda membuat konektor, Security Hub mulai memantau lingkungan Azure Anda. Anda dapat memeriksa status konektor di halaman Integrasi.

Sesuaikan ruang lingkup konektor Azure

Setelah Anda membuat konektor Microsoft Azure, Anda dapat menyesuaikan cakupan konektor dengan mengubah Langganan Azure atau Wilayah Azure yang dipantau. Perubahan cakupan biasanya berlaku dalam waktu 15—30 menit untuk sumber daya dengan peristiwa Log Aktivitas. Evaluasi penuh Langganan Azure yang baru ditambahkan dapat memakan waktu hingga 24 jam.

Sebelum Anda menyesuaikan cakupan konektor, perhatikan hal berikut:

- Saat Anda mengubah cakupan konektor di Hub Keamanan, konektor terkait layanan terkait di Security Hub CSPM dan Amazon Inspector diperbarui secara otomatis agar sesuai.
- Cakupan konektor Hub Keamanan tidak boleh kurang dari konektor yang dikelola pelanggan yang ada di Security Hub CSPM atau Amazon Inspector untuk penyewa Azure yang sama.
- Jika Anda menambahkan Wilayah ke cakupan konektor, Anda harus menjalankan kembali skrip penyiapan untuk menyediakan infrastruktur Event Hub di Wilayah baru. Konfigurasi Event Hub Anda yang ada tidak terpengaruh.

Verifikasi kesehatan konektor Azure

Anda dapat memeriksa kesehatan konektor Microsoft Azure kapan saja untuk mengonfirmasi bahwa Hub Keamanan menerima data dari lingkungan Azure Anda.

Untuk memverifikasi kesehatan konektor

1. Buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/advanced/home? wilayah = us-east-1. .
2. Di panel navigasi, pilih Integrasi dan pilih konektor Azure Anda.
3. Verifikasi bahwa status konektor menunjukkan Aktif. Jika konektor menunjukkan Aktif, verifikasi selesai. Jika itu menunjukkan status yang berbeda, lihatthe section called “Memecahkan masalah konektor”.
4. Arahkan ke Temuan dan filter berdasarkan `ResourceCloudProviders = Azure` untuk mengonfirmasi bahwa temuan sedang dibuat untuk sumber daya Azure Anda.
5. Periksa halaman Standar keamanan untuk mengonfirmasi bahwa standar CIS Azure v4.0 menunjukkan kontrol dalam status PASSED atau FAILED (tidak semua NO_DATA).

> **Note**
>
> Status kesehatan konektor akhirnya konsisten. Ketika masalah izin atau konfigurasi terjadi, status konektor berubah menjadi Ter degradasi dengan cepat dengan pesan yang dapat ditindaklanjuti. Namun, setelah Anda memperbaiki masalah, status dapat memakan waktu hingga 24 jam untuk kembali ke Ter hubung.
>
> - Status ter degradasi setelah perbaikan terbaru tidak selalu menunjukkan masalah yang sedang berlangsung.

- Untuk visibilitas real-time terhadap kegagalan perekaman, periksa CloudWatch metrik di namespace.

Memecahkan masalah konektor Azure

Jika Anda mengalami masalah dengan konektor Anda, tinjau masalah umum dan resolusi berikut.

Status konektor tidak sehat

Masalah ini biasanya terjadi jika kredenSIAL federasi tidak dikonfigurasi dengan benar di Azure.

Untuk mengatasi masalah ini, verifikasi bahwa URL Penerbit Token dan ARN subjek di kredenSIAL federasi Azure Anda cocok dengan Anda Akun AWS.

Tidak ada temuan setelah 30 menit

Masalah ini dapat terjadi jika Event Hub tidak menerima Log Aktivitas.

Untuk mengatasi masalah ini, periksa apakah pengaturan diagnostik dikonfigurasi pada langganan Azure Anda dan bahwa namespace Event Hub diberi tag dengan `AWSConfig-`*`account-id`*`-`*`region`* benar.

Semua kontrol menunjukkan NO_DATA

Masalah ini dapat terjadi jika konektor dinonaktifkan atau jika AWS Config tidak dapat mencapai lingkungan Azure Anda.

Untuk mengatasi masalah ini, verifikasi bahwa konektor diaktifkan dan bahwa prinsipal layanan memiliki peran Pembaca di lingkup grup manajemen root penyewa.

Tidak dapat merekam beberapa sumber daya Azure

Kesalahan dapat terjadi karena salah satu alasan berikut:

- Lingkungan Azure tidak memenuhi prasyarat untuk perekaman sumber daya.
- Pendaftaran aplikasi tidak memiliki persetujuan admin untuk izin Microsoft Graph API.
- Penetapan peran Pembaca tidak mencakup semua cakupan yang diperlukan.
- Penyewa Microsoft Entra ID tidak memiliki data log yang diperlukan.

Untuk mengatasi kesalahan, lakukan hal berikut:

1. Untuk mengonfirmasi bahwa lingkungan Anda memenuhi semua persyaratan, tinjau Pr asyarat untuk Microsoft Azure.

2. Konfirmasikan bahwa pendaftaran aplikasi memiliki izin Microsoft Graph API yang diperlukan dengan persetujuan admin.
3. Verifikasi bahwa prinsipal layanan memiliki peran Pembaca di lingkup grup manajemen root penyewa.

Temuan hanya muncul untuk beberapa langganan

Masalah ini dapat terjadi jika ekspor Log Aktivitas tidak dikonfigurasi untuk semua langganan target.

Untuk mengatasi masalah ini, konfirmasikan bahwa pengaturan diagnostik mencakup semua langganan yang termasuk dalam cakupan konektor.

Bagaimana Security Hub menangani sumber daya dan menemukan pengidentifikasi

Dengan mengaktifkan integrasi Azure Anda untuk Hub AWS Keamanan, pengidentifikasi pencarian sumber daya dan keamanan dari penyedia cloud lain disimpan di AWS Config, Hub Keamanan, dan AWS layanan lain (sesuai kebutuhan) sebagai metadata yang terkait dengan pengelolaan konfigurasi sumber daya yang sesuai dan data pencarian keamanan yang dikumpulkan dari penyedia cloud lainnya. Pengidentifikasi tersebut bukan merupakan Konten Anda. Jangan menyertakan informasi sensitif, rahasia, atau identitas pribadi di dalamnya.

Pengidentifikasi berikut dari lingkungan cloud yang terhubung disimpan dan digunakan AWS untuk menyediakan kemampuan keamanan multicloud:

- Pengidentifikasi sumber daya: ID Penyewa Azure, ID Langganan, Lokasi (wilayah), ID Sumber Daya (ID atau Nama Grup Sumber Daya, Penyedia Sumber Daya, Jenis Sumber Daya)
- Pengidentifikasi Penemuan Keamanan: pengidentifikasi unik yang ditetapkan untuk setiap temuan keamanan yang dihasilkan oleh layanan pendeteksi.

Hubungan antara pengidentifikasi ini - termasuk bagaimana sumber daya berhubungan satu sama lain dan bagaimana temuan berhubungan dengan sumber daya - juga disimpan sebagai metadata layanan. AWS menggunakan pengidentifikasi ini untuk korelasi sumber daya, mengaitkan temuan dengan sumber daya, pencatatan operasional layanan, dan de-duplikasi.

Menghapus konektor Microsoft Azure di Hub Keamanan

Setelah Anda membuat konektor Microsoft Azure di Hub AWS Keamanan, Anda dapat menghapusnya kapan saja. Jika Anda menghapus konektor, Security Hub berhenti melakukan

pemeriksaan manajemen postur dan pemantauan kerentanan untuk lingkungan Azure Anda. Security Hub juga berhenti menghasilkan temuan baru dan data lain tentang lingkungan Anda. Temuan Anda yang ada disimpan selama 90 hari. Inventaris sumber daya tetap seperti saat konektor dihapus dan dihapus setelah 90 hari.

Saat Anda menghapus konektor, Security Hub secara otomatis menghapus konektor terkait layanan terkait di AWS Security Hub CSPM dan Amazon Inspector. Security Hub tidak menghapus pendaftaran aplikasi Azure dan infrastruktur Event Hub di lingkungan Azure Anda. Anda harus menghapus ini secara manual, langsung di Microsoft Azure. Untuk mempelajari caranya, lihat Mengh apus aplikasi di dokumentasi Microsoft Azure.

Untuk menghapus konektor Azure

1. Buka konsol Hub AWS Keamanan di https://console.aws.amazon.com/securityhub/advanced/home? wilayah = us-east-1. .
2. Di panel navigasi, pilih Integrasi.
3. Pilih konektor yang ingin Anda hapus.
4. Pilih Hapus.
5. Saat diminta, konfirmasikan bahwa Anda ingin menghapus konektor.

> **Important**
>
> Jika Anda menghapus konektor dan membuat konektor baru dalam waktu 6 jam, deteksi sumber daya mungkin memakan waktu hingga 6 jam. Rencanakan penghapusan konektor dan rekreasi yang sesuai.

Bekerja di dasbor ringkasan di Hub Keamanan

Das bor Ringkasan di konsol Hub Keamanan menampilkan ikhtisar eksposur, ancaman, sumber daya, dan cakupan keamanan Anda di seluruh widget keamanan. Anda dapat menyesuaikan dasbor dengan menambahkan dan menghapus widget dan dengan membuat dan menerapkan set filter untuk mengambil data di setiap widget.

Pertimbangan-pertimbangan

Pertimbangkan hal berikut sebelum berinteraksi dengan dasbor:

- Kustomisasi seperti set filter yang disimpan atau perubahan tata letak widget disimpan secara otomatis.
- Data secara otomatis disegarkan setiap kali Anda membuka dasbor.
- Jika Anda mengonfigurasi agregasi lintas wilayah, dasbor menyertakan temuan dari semua Wilayah tertaut Anda (saat melihat dasbor di Wilayah rumah Anda).

Pertimbangkan hal berikut jika akun Anda adalah akun administrator yang didelegasikan untuk organisasi, akun anggota dalam organisasi, atau akun mandiri.

- Penyesuaian yang dibuat oleh akun administrator yang didelegasikan akan disimpan secara independen dari penyesuaian yang dilakukan oleh akun anggota. Penyesuaian mungkin termasuk set filter yang disimpan atau perubahan tata letak widget.
- Jika akun Anda adalah akun administrator yang didelegasikan untuk suatu organisasi, data mencakup temuan untuk akun dan akun anggota Anda.
- Jika akun Anda adalah akun anggota di organisasi atau akun mandiri, data hanya mencakup temuan untuk akun Anda.

Sebagai praktik terbaik, jangan sertakan informasi rahasia, sensitif, atau identitas pribadi (PII) dalam kumpulan filter yang disimpan, widget khusus, atau bidang teks bentuk bebas terkait lainnya.

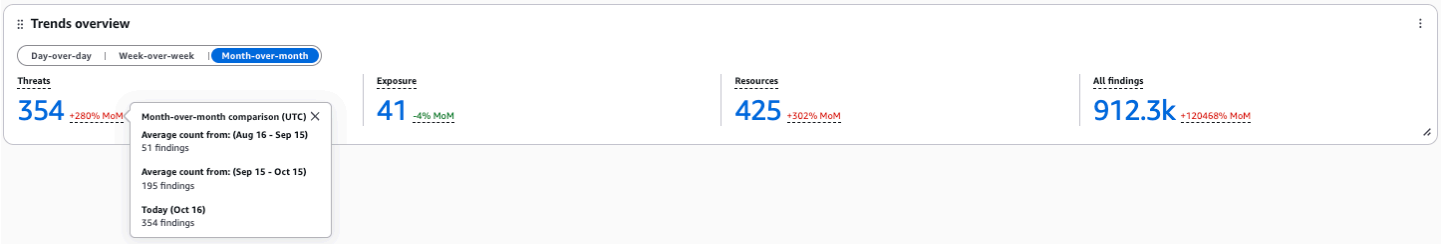
Widget yang tersedia

Anda dapat berinteraksi dengan widget yang berbeda di tab Eksekutif dan Triage di dasbor Ring kasan. Tab Eksekutif mencakup widget yang menampilkan data tren untuk eksposur, ancaman, dan sumber daya Anda dan widget Cakupan Keamanan untuk membantu melacak cakupan akun Anda di berbagai kemampuan keamanan. Tab Triage menyertakan widget yang menampilkan ringkasan eksposur, ancaman, dan sumber daya Anda. Namun, Anda dapat menambahkan widget, menghapus widget, dan mengelola posisi setiap widget di kedua tab untuk menyesuaikan pengalaman Anda.

Widget tren

Widget berikut menampilkan data tren untuk eksposur, ancaman, dan sumber daya Anda, sehingga Anda dapat menganalisisnya dari waktu ke waktu.

Widget ikhtisar tren



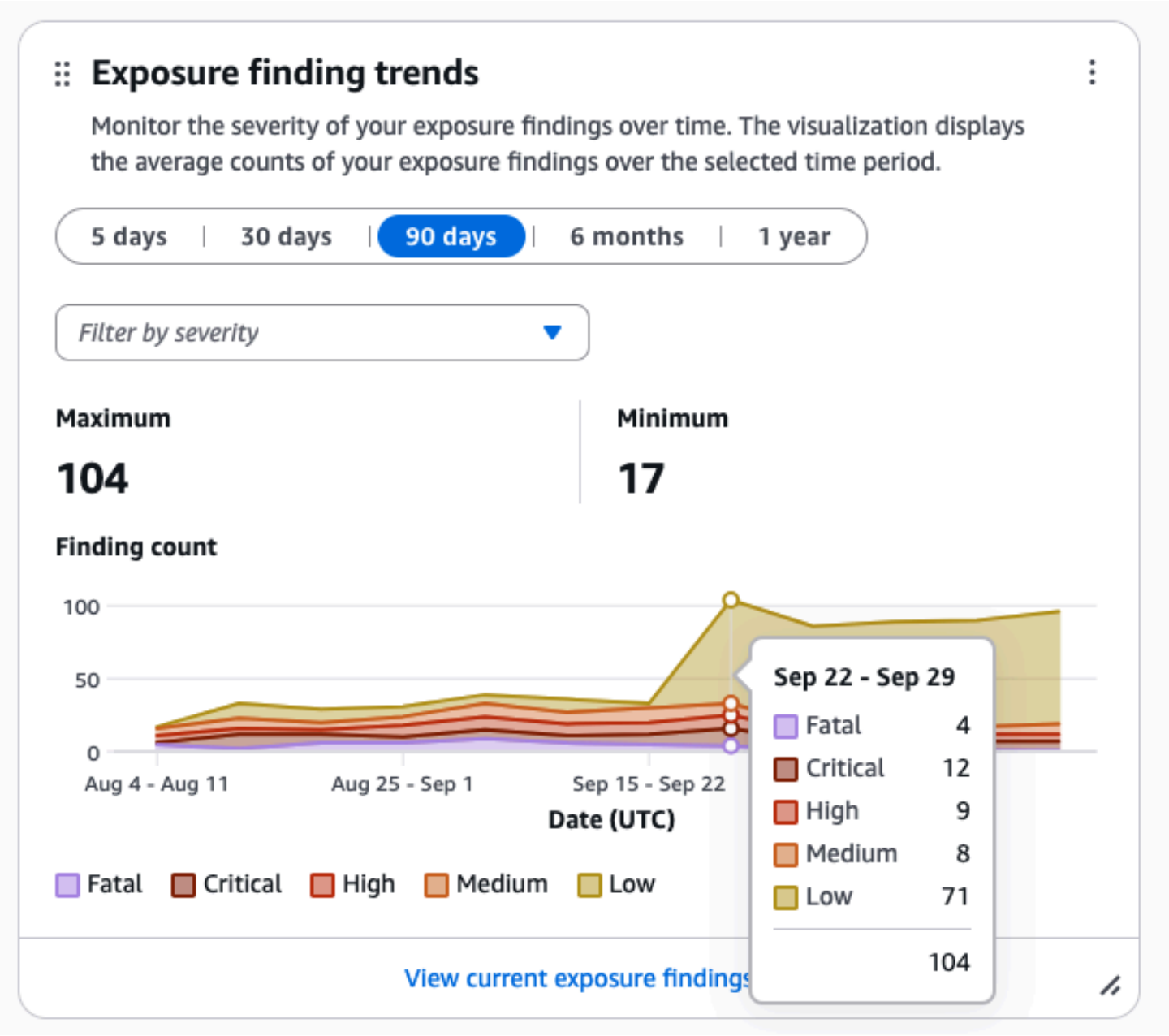
Widget ini menampilkan ikhtisar eksposur, ancaman, sumber daya, dan temuan Anda dalam periode waktu berikut:

- Month-over-monthmencerminkan penghitungan periode-over-periode selama dua bulan terakhir.
- Week-over-weekmencerminkan penghitungan periode-over-periode selama dua minggu terakhir.
- Day-over-daymencerminkan penghitungan periode-over-periode selama 2 hari terakhir.

Angka di sebelah persentase mencerminkan penghitungan periode-over-periode rata-rata hingga saat ini. Memilih nomor ini mengarahkan Anda ke dasbor yang sesuai di konsol. Jika Anda menavigasi ke dasbor lain yang menampilkan data tren, dasbor hanya menampilkan data tren selama 90 hari terakhir atau dalam periode waktu yang paling sesuai jika akun Anda tidak berisi temuan atau sumber daya yang lebih tua dari 30 hari.

> **Note**
>
> Untuk menerima data di widget ini, Anda harus mengaktifkan layanan keamanan berikut:
>
> - AWS Security Hub CSPM — Untuk menerima data tentang eksposur
> - Amazon Inspector - Untuk menerima data tentang eksposur
> - GuardDuty— Untuk menerima data tentang ancaman

Widget tren pencarian eksposur



Widget ini menampilkan tingkat keparahan temuan eksposur Anda dalam periode waktu berikut:

- 5 hari
- 30 hari
- 90 hari
- 6 bulan
- 1 tahun

Visualisasi menampilkan jumlah rata-rata temuan Anda selama periode waktu yang dipilih.

Filter tingkat keparahan

Anda dapat memperbarui grafik dengan menyertakan atau mengecualikan filter tingkat keparahan berikut:

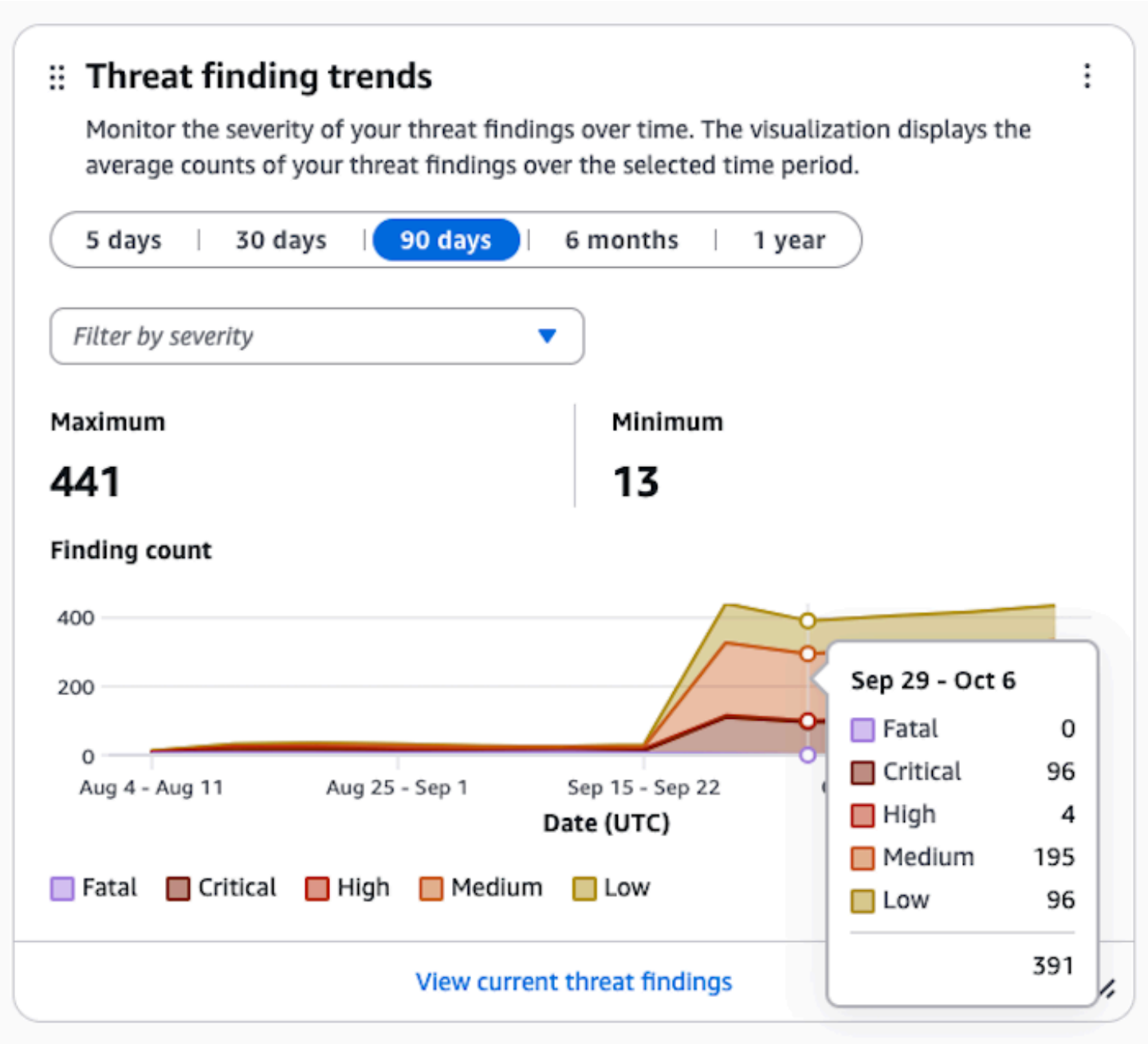
- Fatal
- Kritis
- Tinggi
- Sedang
- Rendah
- Informasi
- Lainnya
- Tidak diketahui

Filter keparahan yang diterapkan ditampilkan di bagian bawah visualisasi di kotak yang berbeda. Anda dapat mengarahkan kursor ke visualisasi untuk meninjau jumlah rata-rata temuan untuk titik waktu tertentu. Anda juga dapat meninjau jumlah rata-rata temuan yang cocok dengan setiap filter tingkat keparahan yang diterapkan.

Anda dapat memilih Lihat semua temuan eksposur saat ini untuk diarahkan ke dasbor Eksposur. Secara default, das bor Eksposur hanya menampilkan data tren selama 90 hari terakhir. Jika akun Anda tidak berisi temuan eksposur yang lebih tua dari 30 hari, dasbor menampilkan data tren berdasarkan periode waktu yang paling sesuai.

> **Note**
>
> Untuk menerima data di widget ini, Anda harus mengaktifkan Amazon Inspector dan Security Hub CSPM.

Widget tren menemukan ancaman



Widget ini menampilkan tingkat keparahan temuan ancaman Anda dalam periode waktu berikut:

- 5 hari
- 30 hari
- 90 hari
- 6 bulan
- 1 tahun

Visualisasi menampilkan jumlah rata-rata temuan Anda selama periode waktu yang dipilih.

Filter tingkat keparahan

Anda dapat memperbarui grafik dengan menyertakan atau mengecualikan filter tingkat keparahan berikut:

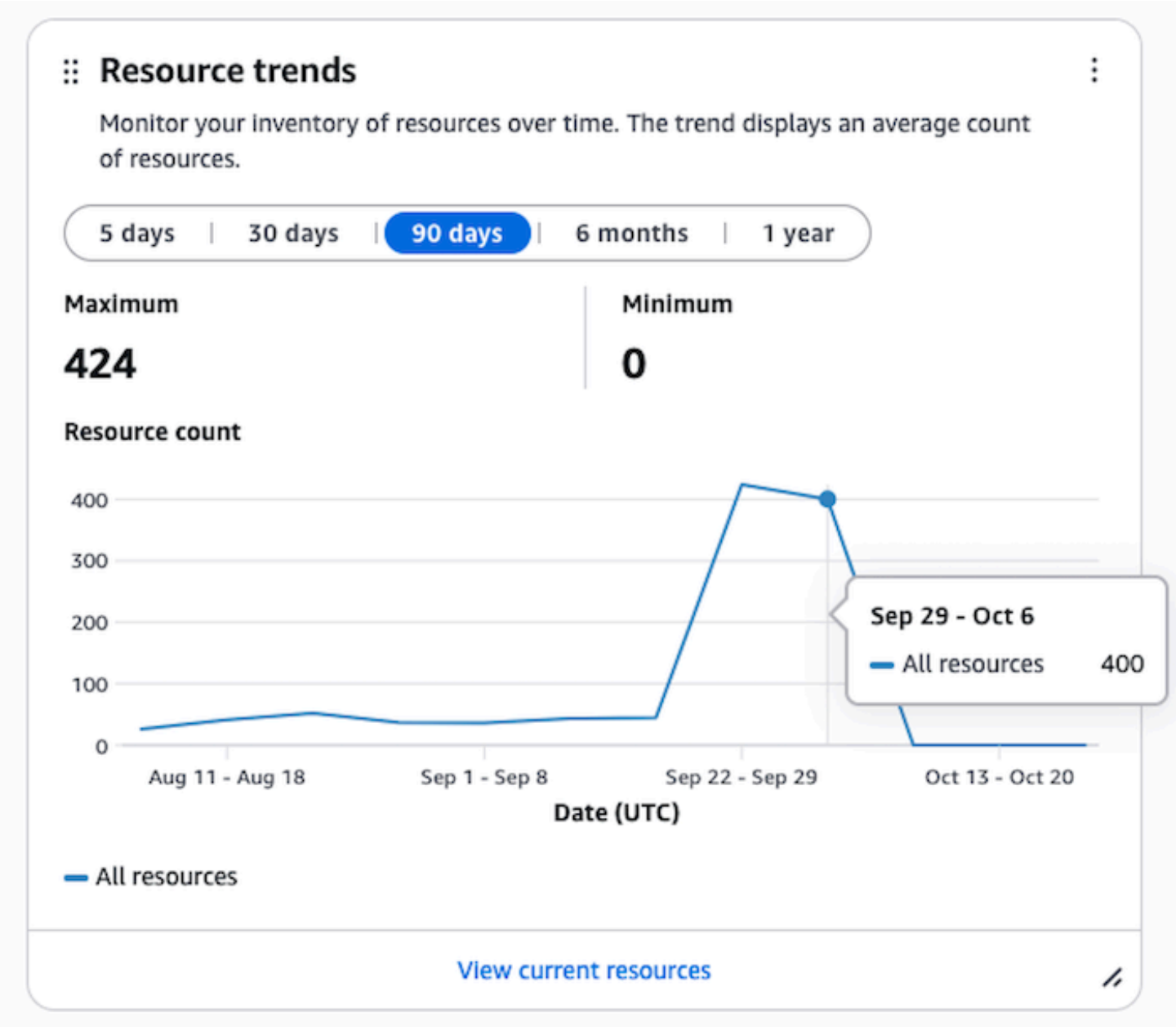
- Fatal
- Kritis
- Tinggi
- Sedang
- Rendah
- Informasi
- Lainnya
- Tidak diketahui

Filter keparahan yang diterapkan ditampilkan di bagian bawah visualisasi di kotak yang berbeda. Anda dapat mengarahkan kursor ke visualisasi untuk meninjau jumlah rata-rata temuan untuk titik waktu tertentu. Anda juga dapat meninjau jumlah rata-rata temuan yang cocok dengan setiap filter tingkat keparahan yang diterapkan.

Anda dapat memilih Lihat semua temuan ancaman saat ini untuk diarahkan ke dasbor Eksposur. Secara default, das bor Ancaman hanya menampilkan data tren selama 90 hari terakhir. Jika akun Anda tidak berisi temuan ancaman yang lebih tua dari 30 hari, dasbor menampilkan data tren berdasarkan periode waktu yang paling sesuai.

> **Note**
>
> Untuk menerima data di widget ini, Anda harus mengaktifkan GuardDuty.

Widget tren sumber daya



Widget ini menampilkan inventaris sumber daya Anda dalam periode waktu berikut:

- 5 hari
- 30 hari
- 90 hari
- 6 bulan
- 1 tahun

Visualisasi menampilkan jumlah rata-rata sumber daya Anda selama periode waktu yang dipilih. Anda dapat mengarahkan kursor ke visualisasi untuk meninjau jumlah rata-rata sumber daya untuk titik waktu tertentu.

Anda dapat memilih Lihat sumber daya saat ini untuk diarahkan ke dasbor Sumber Daya. Secara default, dasbor Sumber daya hanya menampilkan data tren selama 90 hari terakhir. Jika akun Anda tidak berisi sumber daya yang lebih tua dari 30 hari, dasbor menampilkan data tren berdasarkan periode waktu yang paling sesuai.

Widget ini menampilkan inventaris sumber daya Anda dalam periode waktu berikut:

- 5 hari
- 30 hari
- 90 hari
- 6 bulan
- 1 tahun

Retensi data untuk tren

Security Hub menyimpan data tren selama satu tahun untuk semua Akun AWS tempat Security Hub diaktifkan. Setelah data tren disimpan selama satu tahun, data tersebut dihapus dari Hub Keamanan.

Data tren untuk administrator yang didelegasikan dan akun mandiri dihapus setelah Hub Keamanan dinonaktifkan, atau jika akun dihentikan.

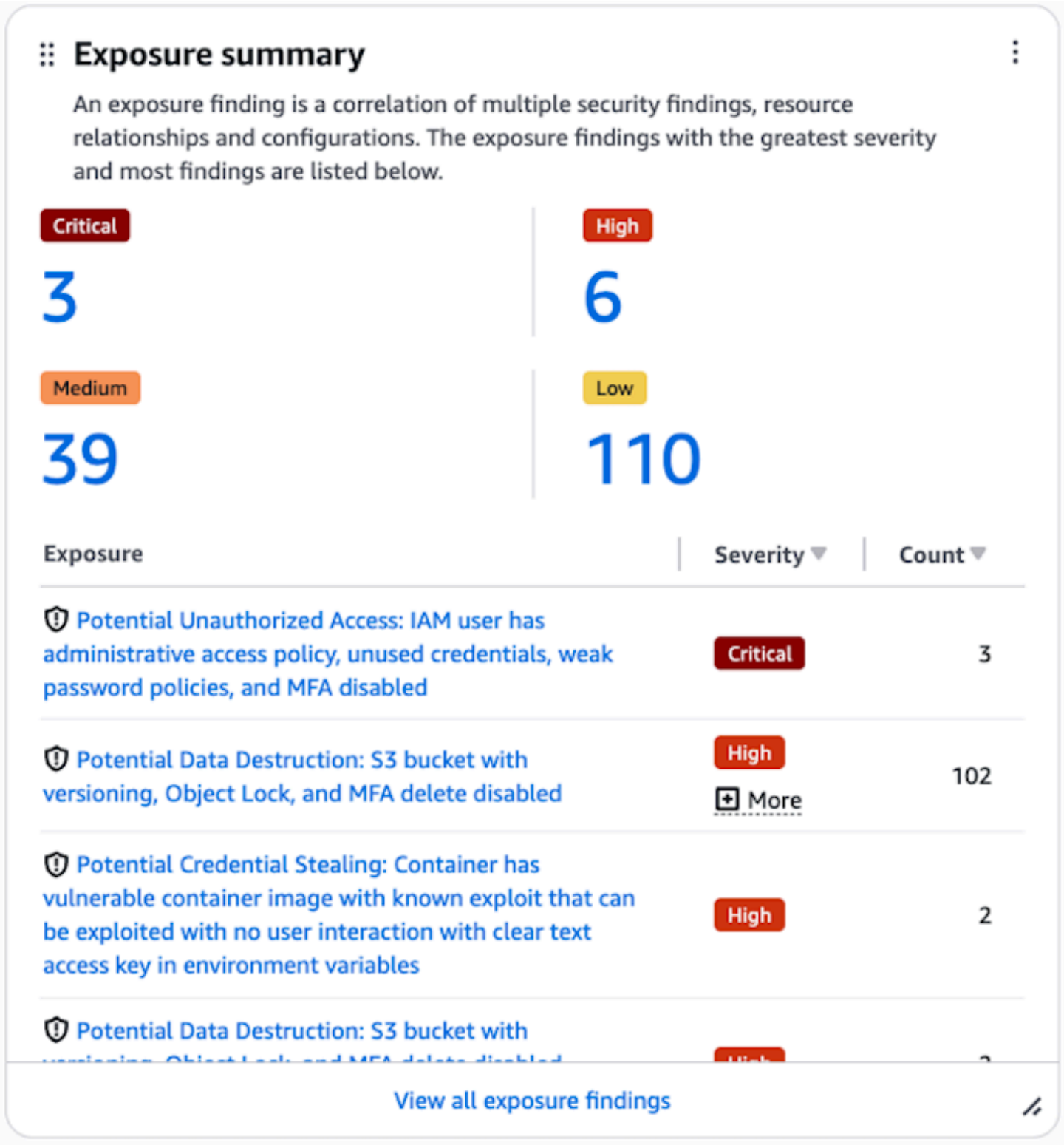
Tren skenario retensi data untuk akun anggota dengan Security Hub diaktifkan:

- Jika akun anggota meninggalkan organisasinya, Security Hub masih menyimpan data tren, hingga saat akun meninggalkan organisasi, selama satu tahun.
- Jika Security Hub dinonaktifkan untuk akun anggota, Security Hub menyimpan data tren, hingga saat akun dinonaktifkan, selama satu tahun.
- Jika akun anggota dihentikan, Security Hub memisahkan data tren dari akun yang dihentikan (misalnya, menghapus ID akun yang dihentikan) dan menyimpan sisa data tren selama satu tahun.

Widget ringkasan

Widget berikut menampilkan ringkasan eksposur, ancaman, dan sumber daya Anda.

Widget ringkasan eksposur

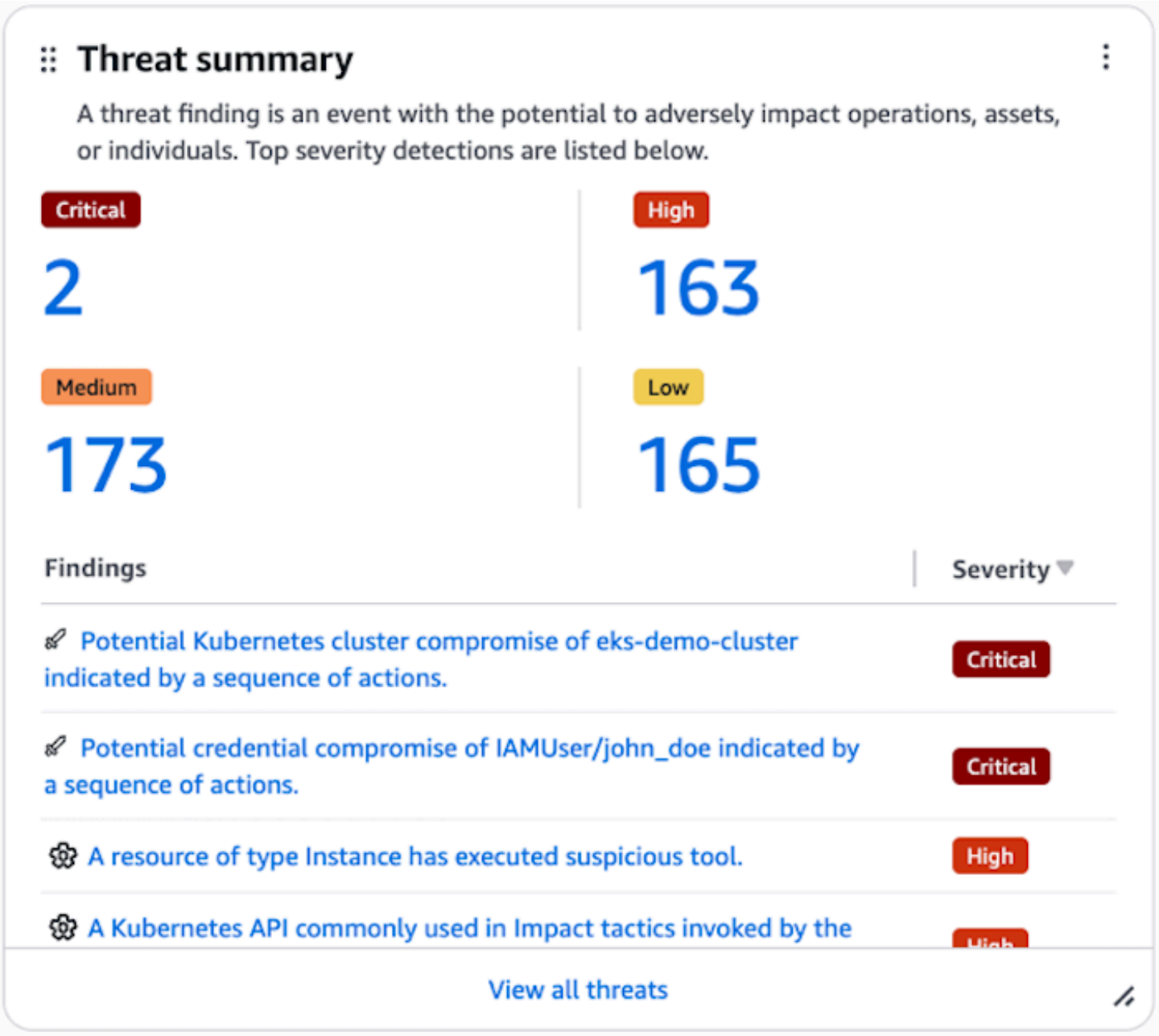


Widget ini menampilkan eksposur Anda berdasarkan tingkat keparahan. Eksposur didasarkan pada analisis temuan dan sifat dari Security Hub dan layanan AWS keamanan lainnya, seperti

Amazon Inspector. Daftar eksposur dalam widget ini terbatas pada delapan eksposur dengan tingkat keparahan tertinggi. Eksposur dengan tingkat keparahan yang lebih besar muncul pertama kali dalam daftar. Jika dua atau lebih eksposur memiliki tingkat keparahan yang sama, daftar secara otomatis mengelompokkan eksposur tersebut di balik eksposur yang lebih baru. Memilih Lihat semua eksposur mengarahkan Anda ke dasbor Eksposur.

> **Note**
>
> Untuk menerima data di widget ini, Anda harus mengaktifkan Amazon Inspector dan Security Hub CSPM.

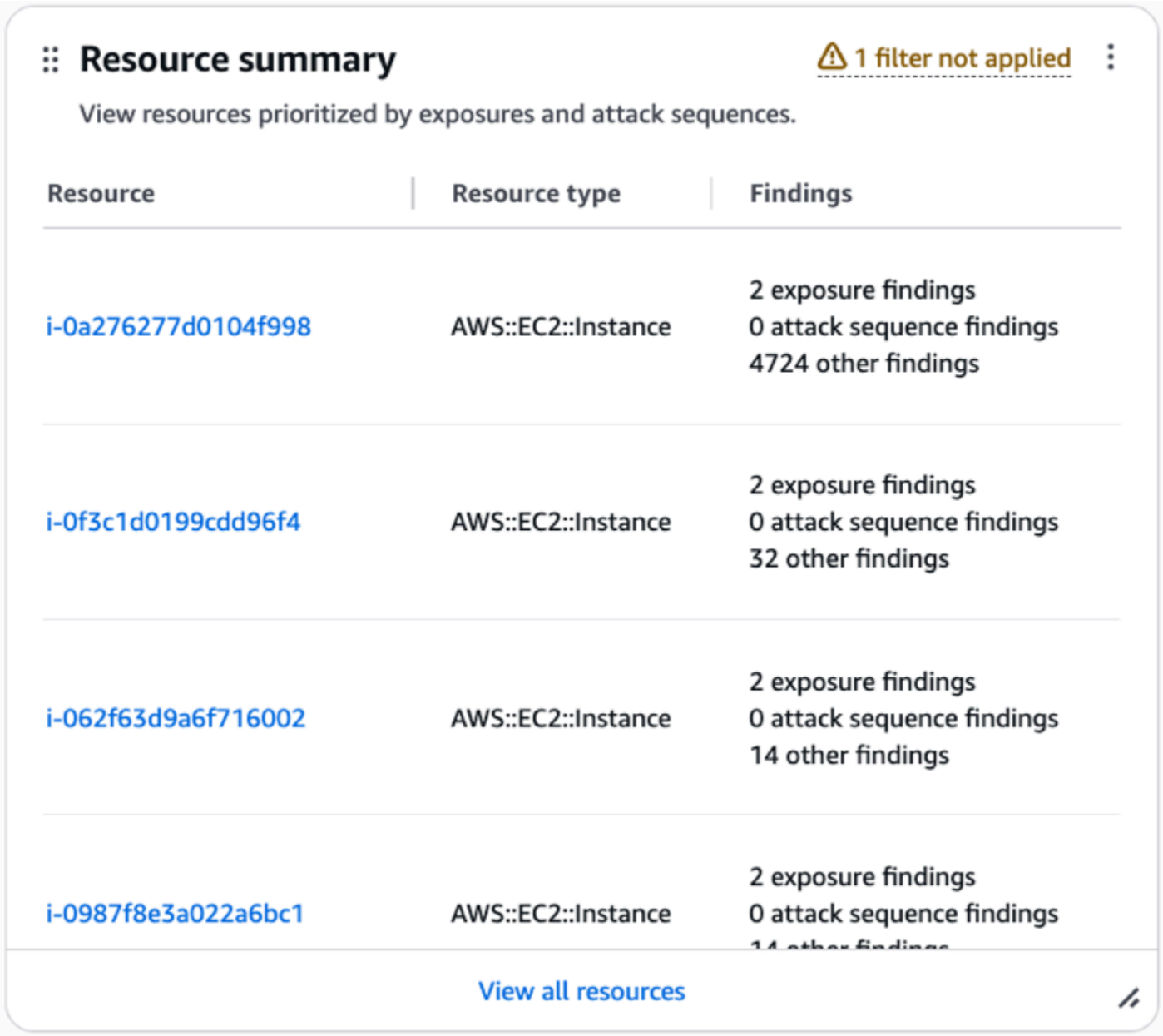
Widget ringkasan ancaman



Widget ini menampilkan ancaman Anda berdasarkan tingkat keparahan. Ancaman mengacu pada aktivitas berbahaya atau aktivitas mencurigakan yang dapat membahayakan keamanan lingkungan Anda. Daftar ancaman dalam widget ini terbatas pada delapan ancaman dengan tingkat keparahan tertinggi. Ancaman dengan tingkat keparahan yang lebih besar muncul pertama kali dalam daftar. Jika dua atau lebih ancaman memiliki tingkat keparahan yang sama, daftar secara otomatis mengelompokkan ancaman tersebut di balik ancaman yang lebih baru. Memilih Lihat semua ancaman mengarahkan Anda ke dasbor Ancaman.

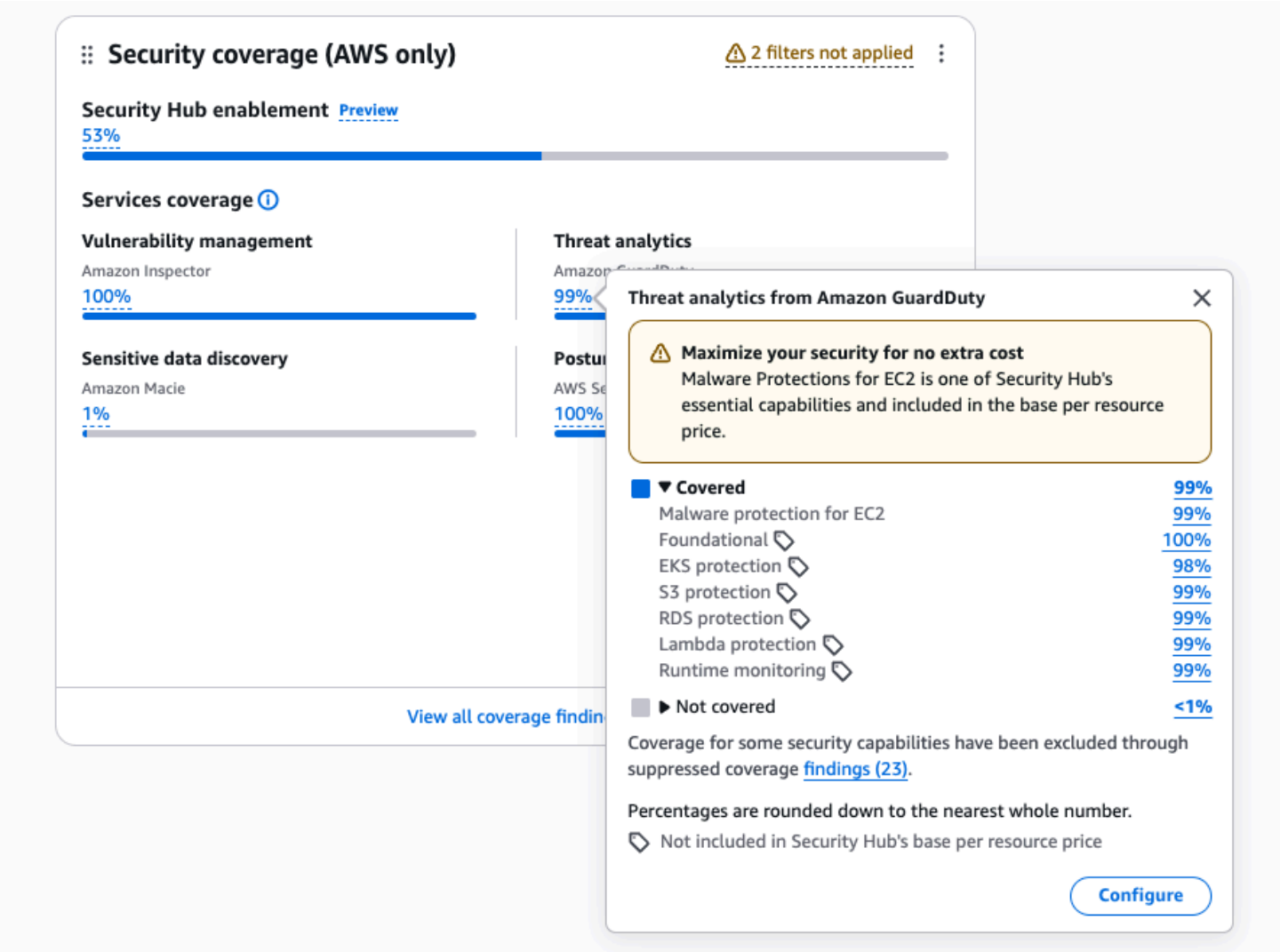
> **Note**
>
> Untuk menerima data di widget ini, Anda harus mengaktifkan GuardDuty.

Widget ringkasan sumber daya



Widget ini menampilkan sumber daya berdasarkan jenis dan temuan yang terkait dengan sumber daya. Sumber daya diprioritaskan oleh eksposur dan urutan serangan. Memilih Lihat semua sumber daya mengarahkan Anda ke dasbor Sumber daya.

Widget cakupan keamanan



Widget menampilkan ringkasan cakupan akun Anda untuk kemampuan keamanan berikut:

- Manajemen kerentanan oleh Amazon Inspector
- Deteksi ancaman oleh Amazon GuardDuty
- Penemuan data sensitif oleh Amazon Macie
- Manajemen postur oleh AWS Security Hub CSPM

Di akun administrator yang didelegasikan, widget juga menampilkan cakupan akun untuk pengaktifan Hub Keamanan.

Setiap item cakupan menunjukkan persentase yang mewakili pengaktifan kemampuan tersebut di seluruh akun Anda. Memilih persentase menampilkan detail tentang cakupan untuk kemampuan itu.

Memilih persentase pengaktifan Hub Keamanan menampilkan panel samping. Panel menunjukkan berapa banyak akun yang diaktifkan di setiap Wilayah di seluruh organisasi Anda.

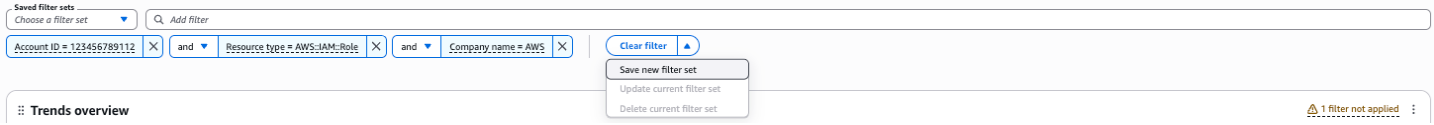
Di bagian C akupan Layanan, persentase mewakili proporsi pemeriksaan cakupan yang dilewati untuk setiap kemampuan keamanan. Pemeriksaan ini mencakup akun dan Wilayah tempat Hub Keamanan diaktifkan. Memilih persentase cakupan menampilkan popover yang memecah setiap fitur sebagai Terc akup (centang lulus) atau Tidak tercakup (centang gagal). Persentase dibulatkan ke bawah ke bilangan bulat terdekat. Memilih persentase apa pun di popover membuka halaman temuan cakupan dengan detail tentang temuan yang membentuk persentase itu. Pilih Konfigurasi untuk membuka layanan individual tempat Anda dapat mengelola konfigurasi untuk kemampuan tersebut, atau untuk membuka halaman konfigurasi Hub Keamanan tempat Anda dapat memperbarui konfigurasi untuk layanan keamanan.

Jika salah satu temuan cakupan Anda di Hub Keamanan ditekan, widget menampilkan pesan yang memberi tahu Anda bahwa cakupan telah dikecualikan: Cak upan untuk kemampuan keamanan telah dikecualikan melalui temuan cakupan yang ditekan.

Untuk informasi selengkapnya tentang melihat dan menekan temuan cakupan, lihat Temuan Cakupan di Hub Keamanan.

Filter yang tersedia

Anda dapat menerapkan filter ke widget keamanan menggunakan bilah Tambah filter.



Filter diatur dalam kategori berikut:

- Filter bersama - berlaku untuk semua widget keamanan
- Menem ukan filter - berlaku untuk widget keamanan yang menampilkan data pencarian
- Filter sumber daya - berlaku untuk widget keamanan yang menampilkan data sumber daya

Anda dapat membuat set filter dengan menghubungkan filter menggunakan operator dan/atau lalu memilih S impan set filter baru di dropdown.

Filter diterapkan ke widget tren pencarian eksposur dan widget tren menemukan ancaman

Saat ini, filter yang didukung untuk widget ini meliputi:

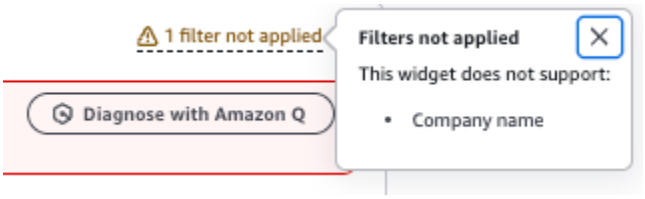
- ID Akun
- Menemukan nama kelas
- Menemukan jenis
- Nama Produk
- Wilayah
- Status

Filter diterapkan ke widget Tren sumber daya

Saat ini, filter yang didukung untuk widget ini meliputi:

- ID Akun
- Wilayah
- Kategori sumber daya
- Tipe sumber daya

Filter tidak diterapkan ke widget



Jika widget tidak mendukung filter, filter tidak diterapkan ke widget. Dalam hal ini, widget menampilkan pesan peringatan yang memberi tahu Anda berapa banyak filter yang tidak diterapkan dan mencantumkan nama filter mana yang tidak didukungnya.

Melihat detail tentang sumber daya di Hub Keamanan

Halaman Sumber daya melacak sumber daya umum di seluruh akun dan organisasi Anda. Anda dapat mengakses halaman Resources di konsol Security Hub dengan memilih Resources di panel navigasi. Manfaat halaman Sumber Daya adalah membantu Anda memantau postur keamanan

Anda, mengatur sumber daya Anda, dan meninjau detail tentang sumber daya Anda. Saat memilih jenis sumber daya, Anda dapat meninjau semua sumber daya yang terkait dengan jenis sumber daya. Anda dapat meninjau temuan apa pun yang terkait dengan sumber daya. Jenis sumber daya yang tersedia di halaman Sumber mencakup sumber daya apa pun di akun Anda yang dicakup oleh layanan AWS keamanan yang berkontribusi temuan ke Hub Keamanan.

> **Note**
>
> Administrator yang didelegasikan dapat melihat semua sumber daya yang terkait dengan akun anggota. Jika Anda mengonfigurasi rumah Wilayah AWS, Anda dapat melihat semua sumber daya di rumah Anda Wilayah AWS dari tautan Wilayah AWS.

Jika Anda memilih sumber daya, Anda dapat meninjau detail untuk sumber daya tersebut. Rincian ini termasuk nama sumber daya, ID, ARN, jenis, dan kategori. Anda dapat meninjau ID akun yang terkait dengan sumber daya, saat sumber daya dibuat (stempel waktu), dan tempat sumber daya dibuat (Wilayah AWS). Anda juga dapat meninjau detail konfigurasi tambahan tentang sumber daya. Rincian ini dapat ditemukan dalam cuplikan JSON yang dapat Anda salin.

Jika Anda beralih dari tab Ikh tis ar ke tab Temuan, Anda dapat meninjau temuan apa pun yang terkait dengan sumber daya. Tab Tem uan menunjukkan nama setiap temuan, jenis setiap temuan, dan tingkat keparahan setiap temuan. Anda dapat mengelompokkan temuan berdasarkan bidang yang berbeda dan mencari temuan menggunakan filter. Jika Anda memilih temuan, Anda dapat meninjau ikhtisar temuan tersebut, yang mencakup informasi tentang kepatuhan dan cara memperbaiki masalah yang terkait dengan temuan tersebut. Tab Sifat menunjukkan setiap sifat yang telah diidentifikasi tentang sumber daya. Anda dapat melihat sifat yang berkontribusi yang digunakan untuk membuat temuan eksposur untuk sumber daya. Anda juga dapat melihat sifat kontekstual, yang merupakan item keamanan lain yang diidentifikasi untuk sumber daya tetapi tidak secara langsung berkontribusi pada temuan paparan apa pun. Jika Anda kembali ke sumber daya, Anda dapat memilih Buka sumber daya untuk meninjau sumber daya di konsol untuk jenis sumber dayanya. Misalnya, jika sumber daya adalah sumber daya IAM, Anda dapat membuka sumber daya di konsol IAM.

Halaman sumber daya memberi Anda berbagai cara untuk mengatur dan mencari sumber daya. Anda dapat mengelompokkan sumber daya berdasarkan jenis. Misalnya, Anda dapat mengelompokkan sumber daya berdasarkan ID akun, jenis pencarian Wilayah AWS, kategori sumber daya, nama sumber daya, dan jenis sumber daya. Filter cepat membantu Anda meninjau sumber daya berdasarkan kategori, akun, dan jenis pencarian.

Hub Keamanan dan Kerangka Kerja Skema Keamanan Siber Terbuka (OCSF)

Security Hub menggunakan Open Cybersecurity Schema Framework (OCSF) sebagai format standar untuk semua temuan keamanan. Topik ini menjelaskan OCSF dan bagaimana Security Hub mengimplementasikannya.

Ikhtisar OCSF

Temuan Security Hub diformat menggunakan OCSF (Open Cybersecurity Schema Framework). OCSF adalah proyek sumber terbuka yang memberikan kerangka kerja yang dapat diperluas untuk mengembangkan skema, bersama dengan skema keamanan inti vendor-agnostik. Vendor dan produsen data lainnya dapat mengadopsi dan memperluas skema untuk domain spesifik mereka. Produsen data dapat memetakan skema yang berbeda untuk membantu tim keamanan menyederhanakan konsumsi dan normalisasi data, sehingga ilmuwan dan analis data dapat bekerja dengan bahasa yang sama untuk deteksi dan penyelidikan ancaman. Tujuannya adalah untuk menyediakan standar terbuka, diadopsi di lingkungan, aplikasi, atau solusi apa pun, sambil melengkapi standar dan proses keamanan yang ada.

Kerangka kerja terdiri dari tipe data, kamus atribut, dan taksonomi. Meskipun tidak terbatas pada keamanan siber atau peristiwa, fokus awalnya adalah pada skema peristiwa keamanan siber. OCSF independen dari format penyimpanan, metode pengumpulan data, dan proses ETL.

Security Hub saat ini mendukung temuan dalam skema OCSF versi 1.6.

Sumber daya terkait

Untuk informasi lebih lanjut tentang OCSF dan implementasinya, lihat sumber daya berikut:

- Dokumentasi OCSF Publik
- Dokumentasi Penggunaan Ekstensi OCSF
- Referensi Skema Inti OCSF
- Registri Ekstensi OCSF

AWS ekstensi untuk OCSF

Skema OCSF dapat diperluas dengan menambahkan atribut, objek, kategori, profil, dan kelas acara baru. Skema adalah agregasi entitas skema inti dan ekstensi.

Ekstensi OCSF memungkinkan vendor atau pelanggan tertentu untuk menambah skema yang ada dengan menambahkan atribut untuk memberikan kustomisasi khusus domain, meningkatkan interoperabilitas data, dan menambahkan konteks yang lebih rinci untuk analisis keamanan.

AWS Ekstensi untuk Kerangka Skema Keamanan Siber Terbuka (OCSF) menyediakan definisi atribut untuk sumber daya cloud dalam acara OCSF. Ekstensi ini menambahkan `cloud_resources` profil yang memperluas `resource_details` objek OCSF dengan atribut sumber daya khusus cloud. Dengan atribut ini, tim keamanan dapat menganalisis konfigurasi sumber daya, potensi kerentanan, dan metadata deteksi ancaman.

Objek **`resource_details yang`** diperluas

Ek AWS stensi memperluas `resource_details` objek dengan atribut yang disebutkan dalam daftar referensi atribut di bawah ini. Atribut ini memastikan identifikasi dan klasifikasi sumber daya cloud yang tepat di seluruh penyedia yang berbeda dalam kerangka acara standar.

AWS Ekstensi untuk referensi atribut OCSF

Bagian Atribut Das_ar_dan objek spesifik sumber daya memberikan contoh masing-masing atribut yang merupakan bagian dari ekstensi AWS OCSF ke resource_details.

Setiap definisi atribut berisi status OCSF yang menguraikan hubungannya saat ini dengan skema OCSF publik:

- Ada: Atribut ini sudah ada di OCSF resource_details standar dan sekarang menjadi bagian dari ekstensi. AWS
- Baru: Atribut bukan bagian dari OCSF dan diperkenalkan sebagai bagian dari AWS ekstensi. Itu tidak ada dalam skema OCSF inti.
- Ditambahkan ke resource_details: Atribut didefinisikan dalam OCSF tetapi bukan bagian dari resource_details.

Atribut dasar

Ini adalah atribut fundamental yang digunakan untuk identifikasi sumber daya, lokasi, dan metadata dasar. Mereka terdiri dari tipe data sederhana seperti string, stempel waktu, dan array.

Partisi awan

Partisi cloud tempat sumber daya ada.

Persyaratan

Disarankan

Tipe

String

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "cloud_partition": "aws"
    }
  ]
}
```

ID akun pemilik

Pengidentifikasi akun 12 digit milik sumber daya.

Persyaratan

Disarankan

Tipe

String

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
```

```
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      }
    }
  ]
}
```

Tipe sumber daya

Jenis AWS CloudFormation sumber daya yang mengidentifikasi layanan dan sumber daya tertentu.

Persyaratan

Diperlukan

Tipe

String

Format

Harus mengikuti konvensi penamaan jenis AWS CloudFormation sumber daya: `AWS::<Service>::<ResourceType>`

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "type": "AWS::EC2::Instance"
    }
  ]
}
```

Pengidentifikasi sumber daya

Pengidentifikasi unik untuk sumber daya cloud (misalnya, i-1234567890abcdef0).

Persyaratan

Disarankan

Tipe

String

Format

Harus merupakan pengidentifikasi sumber daya yang valid. Panjang minimum 1. Panjang maksimum 768.

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "uid": "i-1234567890abcdef0"
    }
  ]
}
```

Pengidentifikasi sumber daya alternatif

Pengidentifikasi unik untuk sumber daya cloud, biasanya Nama Sumber Daya Amazon (ARN).

Persyaratan

Disarankan

Tipe

String

Format

Harus menjadi ARN yang AWS valid. Pola umum meliputi:

- `"arn:partition:service:region:account-id:resource-id"`
- `"arn:partition:service:region:account-id:resource-type/resource-id"`
- `"arn:partition:service:region:account-id:resource-type:resource-id"`

Catatan: Beberapa layanan seperti S3 menggunakan variasi seperti arn:aws:s3: ::bucket-name (tanpa region atau akun-id).

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
    }
  ]
}
```

```
{
  "resources": [
    {
      "uid_alt": "arn:aws:s3:::my-bucket-name"
    }
  ]
}
```

Nama sumber daya

Nama unik untuk sumber daya cloud.

Persyaratan

Disarankan

Tipe

String

Format

User-created nama yang nilainya akan tergantung pada lingkungan.

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "name": "My-Server-1"
    }
  ]
}
```

Wilayah awan

Wil AWS ayah tempat sumber daya berada.

Persyaratan

Disarankan

Tipe

String

Format

Pengidentifikasi wilayah awan yang valid (misalnya, us-east-1, eu-west-1, ap-southeast-2)

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "region": "us-west-2"
    }
  ]
}
```

Waktu pembuatan sumber daya

Waktu ketika sumber daya dibuat.

Persyaratan

Disarankan

Tipe

Stempel waktu

Format

Stempel waktu Unix dalam milidetik sejak zaman (1 Januari 1970, 00:00:00 UTC)

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "created_time": 1762019193000
    }
  ]
}
```

Tanda

Key-value pasangan untuk metadata sumber daya dan organisasi.

Persyaratan

Disarankan

Tipe

Array objek kunci:nilai

Format

Objek generik yang memungkinkan untuk menentukan pasangan kunci:nilai.

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "tags": [
        {
          "name": "Environment",
          "value": "Production"
        },
        {
          "name": "Owner",
          "value": "SecurityTeam"
        }
      ]
    }
  ]
}
```

Alamat IP

Alamat IP yang terkait dengan instance dalam format IPv4 atau IPv6.

Persyaratan

Opsional

Tipe

String

Format

Alamat IPv4 atau IPv6 yang valid

Status OCSF

yang sudah ada

Contoh

```
{
  "resources": [
    {
      "ip": "10.0.1.25"
```

```
    }
  ]
}
```

Alamat IP

Array alamat IP (IPv4 atau IPv6) yang terkait dengan perangkat. Ini mungkin termasuk alamat IP publik dan pribadi.

Persyaratan

Opsional

Tipe

Array alamat IP

Status OCSF

Baru

Contoh

```
{
  "resources": [
    {
      "ip_addresses": ["10.0.1.25", "52.12.34.56"]
    }
  ]
}
```

VPC UID

ID VPC tempat sumber daya berada.

Persyaratan

Opsional

Tipe

String

Format

Pengidentifikasi VPC (misalnya, vpc-12345678900)

Status OCSF

Ditambahkan ke `resource_details`

Contoh

```
{
  "resources": [
    {
      "vpc_uid": "vpc-0a1b2c3d4e5f6g7h8"
    }
  ]
}
```

Contoh objek sumber daya dengan atribut dasar

```
{
  "resources": [
    {
      "cloud_partition": "aws",
      "owner": {
        "account": {
          "uid": "123456789012"
        }
      },
      "region": "us-east-1",
      "type": "AWS::EC2::NetworkInterface",
      "uid": "eni-03e6c892dd45e836c",
      "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-03e6c892dd45e836c",
      "zone": "us-east-1f",
      "vpc_uid": "vpc-0ef6045717b0362f6"
    }
  ]
}
```

Objek khusus sumber daya

Ini adalah objek bersarang kompleks yang memberikan informasi terperinci untuk jenis sumber daya dan layanan tertentu. Setiap objek berisi beberapa bidang dan sub-objek dengan konfigurasi dan metadata khusus layanan.

Perangkat

Atribut instance cloud yang disempurnakan untuk sumber daya komputasi termasuk detail enkripsi, informasi gambar, profil instans, dan waktu peluncuran.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Ditambahkan ke`resource_details`. Lihat definisi objek Perangkat OCSF.

AWS Ekstensi menambahkan atribut berikut ke objek ini:

- `encryption_details`- Rincian enkripsi sumber daya
- `image`- Informasi gambar
- `instance_profile`- Profil instance IAM untuk dikaitkan dengan instance
- `launch_time`- Waktu instance diluncurkan
- `uid_alt`- Nama Sumber Daya Amazon (ARN) dari sumber daya

Contoh


```
{
  "device": {
    "image": {
      "uid": "ami-99999999",
      "name": "LoadTestAMI-Current"
    },
    "instance_profile": {
      "uid": "LoadTestingInstanceProfileId",
      "uid_alt": "arn:aws:iam::012345678999:instance-profile/generated"
    },
    "launch_time": 1762019193000,
    "launch_time_dt": "2025-08-02T02:05:06Z",
    "model": "m3.xlarge",
```

```
    "network_interfaces": [
      {
        "ip": "198.51.100.0",
        "security_groups": [
          {
            "name": "LoadTestingSecurityGroupName",
            "uid": "LoadTestingSecurityId"
          }
        ],
        "uid": "eni-abcdef12"
      }
    ],
    "type": "Virtual",
    "type_id": 6,
    "uid": "i-99999999"
  }
}
```

Antarmuka jaringan

Detail antarmuka jaringan dan konfigurasi termasuk lampiran dan grup keamanan.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Ditambahkan ke`resource_details`. Lihat definisi objek Antarmuka Jaringan OCSF.

AWS Ekstensi menambahkan atribut berikut ke objek ini:

- `attachments`- Informasi tentang lampiran antarmuka jaringan
- `security_groups`- Array pengidentifikasi unik grup keamanan
- `uid_alt`- Nama Sumber Daya Amazon (ARN) dari sumber daya

Contoh

```
{
  "network_interface": {
    "uid": "eni-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:network-interface/
eni-0a1b2c3d4e5f6g7h8",
    "name": "prod-web-server-eni",
    "attachments": [
      {
        "uid": "eni-attach-0abcd1234efgh5678",
        "instance_uid": "i-0123456789abcdef0",
        "name": "/dev/eth0",
        "state": "attached",
        "attach_time": 1762019193000
      }
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "web-server-sg"
      },
      {
        "uid": "sg-9i8h7g6f5e4d3c2b1",
        "name": "ssh-access-sg"
      }
    ]
  }
}
```

Perangkat penyimpanan

Detail perangkat penyimpanan termasuk lampiran, enkripsi, dan informasi snapshot.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Baru

Objek perangkat penyimpanan mencakup atribut berikut:

- `name`- Nama perangkat penyimpanan
- `uid`- Pengidentifikasi unik dari perangkat penyimpanan
- `attachments`- Lampiran perangkat penyimpanan
- `encryption_details`- Kunci enkripsi perangkat penyimpanan
- `is_encrypted`- Apakah perangkat penyimpanan dienkripsi (wajib)
- `snapshot_id`- Pengidentifikasi snapshot perangkat penyimpanan
- `uid_alt`- Nama Sumber Daya Amazon (ARN) dari sumber daya

Contoh

```
{
  "storage_device": {
    "is_encrypted": false,
    "name": "LocalVolumeDeviceName1",
    "snapshot_id": "snap-12345678901234567",
    "uid": "vol-09d5050dea915943d",
    "uid_alt": "arn:aws:ec2:us-west-2:123456789000:volume/vol-09d5050dea915943d"
  }
}
```

Basis Data

Atribut instance database termasuk jenis mesin, titik akhir, dan informasi pengguna.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Ditambahkan `keresource_details`. Lihat definisi objek Database OCSF.

AWS Ekstensi menambahkan atribut berikut ke objek ini:

- `cluster_uid`- Pengidentifikasi cluster database
- `db_endpoint`- Titik akhir database
- `encryption_details`- Rincian enkripsi database
- `engine`- Nama mesin database (misalnya, mysql)
- `is_encrypted`- Apakah database dienkripsi
- `is_iam_authentication`- Apakah otentikasi IAM diaktifkan
- `is_public`- Apakah database dapat diakses publik
- `port`- Nomor port database
- `security_groups`- Array grup keamanan VPC yang terkait dengan instance database
- `snapshot_details`- Rincian snapshot database
- `status`- Status database (misalnya, tersedia)
- `subnet_group`- Grup subnet database adalah kumpulan subnet dalam VPC
- `uid_alt`- Nama Sumber Daya Amazon (ARN) dari sumber daya
- `user`- Pengguna database
- `version`- Versi database

Contoh

```
{
  "database": {
    "cluster_uid": "SampleDBClusterId",
    "engine": "mysql",
    "is_iam_authentication": true,
    "is_public": false,
    "type": "Relational",
    "type_id": 1,
    "uid": "SampleDBId",
    "version": "13.6"
  }
}
```

Cluster database

Atribut instance database termasuk jenis mesin, titik akhir, dan informasi pengguna.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Baru

Objek database mencakup atribut berikut:

- `uid`- Pengidentifikasi unik dari cluster database
- `uid_alt`- Nama Sumber Daya Amazon (ARN) dari sumber daya
- `name`- Nama cluster database
- `status`- Status cluster database
- `engine`- Mesin yang terkait dengan cluster
- `version`- Versi cluster database
- `cluster_members`- Daftar instance database yang merupakan bagian dari cluster
- `security_groups`- Array grup keamanan yang terkait dengan cluster
- `is_encrypted`- Apakah cluster database dienkripsi
- `is_iam_authentication`- Apakah otentikasi IAM diaktifkan
- `encryption_details`- Rincian enkripsi cluster database
- `subnet_group`- Grup subnet yang terkait dengan cluster
- `port`- Nomor port cluster database
- `zones`- Daftar zona ketersediaan
- `db_endpoint`- Titik akhir cluster database
- `snapshot_details`- Rincian snapshot database

Contoh

```
{
```

```
  "db_cluster": {
    "uid": "production-aurora-cluster",
    "uid_alt": "arn:aws:rds:us-east-1:123456789012:cluster:production-aurora-cluster",
    "name": "production-aurora-cluster",
    "status": "available",
    "engine": "aurora-mysql",
    "version": "8.0.mysql_aurora.3.04.0",
    "cluster_members": [
      "instance-1",
      "instance-2"
    ],
    "security_groups": [
      {
        "uid": "sg-0a1b2c3d4e5f6g7h8",
        "name": "db-security-group"
      }
    ],
    "is_encrypted": true,
    "is_iam_authentication": true,
    "encryption_details": {
      "key_uid": "arn:aws:kms:us-
east-1:123456789012:key/12345678-1234-1234-1234-123456789012"
    },
    "subnet_group": {
      "uid": "production-db-subnet-group"
    },
    "port": 3306,
    "zones": [
      "us-east-1a",
      "us-east-1b",
      "us-east-1c"
    ],
    "db_endpoint": {
      "name": "production-aurora-cluster.cluster-abc123xyz.us-
east-1.rds.amazonaws.com",
      "port": 3306
    }
  }
}
```

Fungsi cloud

Atribut fungsi cloud untuk fungsi tanpa server termasuk handler, lapisan, dan konfigurasi runtime.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Baru

Objek fungsi cloud mencakup atribut berikut:

- `name`- Nama fungsi cloud
- `uid`- Pengidentifikasi unik dari fungsi cloud
- `uid_alt`- Nama Sumber Daya Amazon (ARN) dari sumber daya
- `encryption_details`- Rincian enkripsi fungsi cloud
- `handler`- Metode dalam kode fungsi yang memproses peristiwa
- `layers`- Daftar lapisan fungsi cloud yang berisi kode tambahan atau data
- `runtime`- Lingkungan khusus bahasa fungsi cloud
- `security_groups`- Array grup keamanan yang terkait dengan fungsi cloud
- `subnet_info_list`- Rincian tentang subnet yang terkait dengan fungsi cloud
- `user`- Detail tentang entitas IAM yang memberikan izin cloud_function untuk mengakses layanan
- `version`- Versi fungsi cloud
- `vpc_uid`- Pengidentifikasi unik VPC jika fungsi cloud ada di VPC

Contoh

```
{
  "cloud_function": {
    "name": "my-lambda-function",
    "uid": "my-lambda-function",
    "uid_alt": "arn:aws:lambda:us-east-1:123456789012:function:my-lambda-function",
    "handler": "index.handler",
    "runtime": "python3.11",
    "version": "$LATEST",
```

```
    "layers": [
      {
        "name": "my-layer",
        "uid_alt": "arn:aws:lambda:us-east-1:123456789012:layer:my-layer:1",
        "version": "1"
      }
    ],
    "security_groups": [
      {
        "name": "lambda-security-group",
        "uid": "sg-0123456789abcdef0"
      }
    ],
    "subnet_info_list": [
      {
        "uid": "subnet-0a1b2c3d4e5f6g7h8"
      }
    ],
    "vpc_uid": "vpc-0ef6045717b0362f6"
  }
}
```

Databucket

Buket S3 atau atribut penyimpanan data.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Ditambahkan ke`resource_details`. Lihat definisi objek OCSF Databucket.

Catatan: Objek ini ditambahkan ke resource_details oleh Ekstensi. AWS Objek inti OCSF Databucket digunakan tanpa atribut tambahan.

Contoh

```
{
  "databucket": {
    "type": "S3",
    "type_id": 1,
    "uid": "my-bucket-name"
  }
}
```

Citra

Informasi gambar untuk sumber daya komputasi termasuk detail platform dan penggunaan.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Ditambahkan ke`resource_details`. Lihat definisi objek Gambar OCSF.

AWS Ekstensi menambahkan atribut berikut ke objek ini:

- `platform`- Platform sistem operasi gambar
- `in_use_count`- Hitung sumber daya menggunakan gambar ini

Contoh

```
{
  "image": {
    "uid": "ami-0abcdef1234567890",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:image/ami-0abcdef1234567890",
    "name": "my-custom-ami",
    "platform": "AMAZON_LINUX_2",
    "in_use_count": 2
  }
}
```

Info subnet

Rincian tentang subnet tempat sumber daya berada.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Baru

Objek info subnet mencakup atribut berikut:

- `uid`- Pengidentifikasi unik dari subnet
- `uid_alt`- Nama Sumber Daya Amazon (ARN) dari sumber daya
- `name`- Nama subnet
- `zone`- Zona ketersediaan
- `ip_count`- Jumlah alamat IP di subnet
- `cidr_block`- Blok CIDR dari subnet
- `is_default`- Apakah ini subnet default
- `is_public`- Apakah subnet dapat diakses publik
- `state`- Keadaan subnet
- `vpc_uid`- ID VPC tempat subnet berada

Contoh

```
{
  "subnet_info": {
    "uid": "subnet-0a1b2c3d4e5f6g7h8",
    "uid_alt": "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-0a1b2c3d4e5f6g7h8",
    "name": "production-web-subnet-1a",
```

```
    "zone": "us-east-1a",
    "ip_count": 251,
    "cidr_block": "10.0.1.0/24",
    "is_default": false,
    "is_public": true,
    "state": "available",
    "vpc_uid": "vpc-0123456789abcdef0"
  }
}
```

Pengguna

Atribut pengguna IAM termasuk profil instans dan kebijakan.

Persyaratan

Opsional

Tipe

Objek

Status OCSF

Ditambahkan ke`resource_details`. Lihat definisi objek Pengguna OCSF.

Objek pengguna mencakup atribut berikut:

- `instance_profiles`- Daftar profil instance yang dilampirkan ke instance cloud
- `policies`- Kebijakan yang menetapkan izin untuk pengguna, grup, peran, dan sumber daya

Contoh

```
{
  "user": {
    "type_id": 1,
    "uid": "AIDACKCEVSQ6C2EXAMPLE",
    "uid_alt": "arn:aws:iam::123456789012:user/developers/john.doe",
    "name": "john.doe",
    "type": "User",
    "groups": [
      {
```

```
        "name": "Developers"
      },
      {
        "name": "ReadOnlyAccess"
      }
    ],
    "policies": [
      {
        "name": "AmazonS3ReadOnlyAccess"
      },
      {
        "name": "AmazonEC2ReadOnlyAccess"
      }
    ]
  }
}
```

Temuan cakupan di Hub Keamanan

Temuan cakupan untuk Security Hub memberikan visibilitas ke fitur AWS keamanan mana yang diaktifkan dan di mana mungkin ada celah dalam cakupan di akun mandiri atau di seluruh akun anggota organisasi. Temuan cakupan saat ini mendukung pelaporan layanan dan fitur mana yang diaktifkan untuk Amazon GuardDuty, Amazon Inspector, Amazon Macie, dan AWS Security Hub CSPM. Temuan ini muncul di widget Cakupan Keamanan di dasbor Security Hub dengan kemampuan untuk menelusuri tampilan yang lebih mendetail dengan kemampuan keamanan tertentu.

Batasan

- Untuk akun anggota, informasi cakupan dikumpulkan di seluruh tautan Wilayah AWS, tetapi hanya untuk akun anggota tersebut.
- Informasi cakupan tidak ditampilkan untuk akun yang tidak masuk ke Hub Keamanan.

Temuan cakupan untuk AWS Hub Keamanan CSPM

Temuan cakupan CSPM Security Hub menilai apakah standar keamanan manajemen postur yang memenuhi syarat diaktifkan di akun. Mengaktifkan Standar CSPM Hub Keamanan apa pun akan memenuhi syarat, dengan pengecualian AWS Control Tower dan standar Penandaan Sumber Daya.

Diperlukan waktu hingga 24 jam untuk mendeteksi standar yang diaktifkan secara default saat mengaktifkan Security Hub CSPM.

Temuan cakupan untuk Amazon GuardDuty

GuardDuty Temuan cakupan menilai GuardDuty apakah diaktifkan dan GuardDuty fitur mana yang diaktifkan di Akun AWS:

- GuardDuty Perlindungan Malware untuk Amazon EC2 — Memindai instans Amazon EC2 untuk malware potensial.
- GuardDuty Perlindungan Amazon EKS — Memantau log audit Kubernetes untuk ancaman di cluster Amazon EKS.
- GuardDuty Perlindungan Lambda — Menganalisis pemanggilan fungsi Lambda untuk potensi ancaman.
- GuardDuty Amazon S3 Protection — Menganalisis peristiwa data untuk potensi ancaman terhadap bucket Amazon S3.
- GuardDuty Perlindungan Amazon RDS — Memantau ancaman terhadap database Amazon RDS.
- GuardDuty Pemantauan Runtime — Menyediakan pemantauan real-time dari perilaku runtime di instans Amazon EC2.
- GuardDuty Cakupan Dasar — GuardDuty Fitur dasar yang secara otomatis diaktifkan saat GuardDuty diaktifkan.

> **Note**
>
> Untuk GuardDuty Cakupan Dasar, temuan cakupan yang menunjukkan fitur dinonaktifkan GuardDuty rata-rata tidak diaktifkan di akun untuk temuan cakupan.

Diperlukan waktu hingga 24 jam agar pembaruan GuardDuty cakupan tercermin di semua akun anggota dalam suatu organisasi.

Temuan cakupan untuk Amazon Inspector

Temuan cakupan Amazon Inspector menilai apakah Amazon Inspector diaktifkan dan fitur mana yang diaktifkan di akun:

- Inspector EC2 Scanning — Memindai instans Amazon EC2 untuk mencari kerentanan.
- Inspector ECR Scanning — Memindai gambar wadah Amazon ECR untuk mencari kerentanan.
- Inspector Lambda Standard Scanning — Memindai fungsi Lambda untuk kerentanan.
- Inspektur Lambda Code Scanning — Memindai fungsi kode Lambda untuk kerentanan kode.

Temuan cakupan untuk Amazon Macie

Temuan cakupan Macie menilai apakah Macie diaktifkan di: Akun AWS

- Cakupan Penemuan Data Sensitif Otomatis Macie — Terus mengevaluasi kekayaan data Amazon S3 Anda untuk data sensitif.

Diperlukan waktu hingga 24 jam untuk pembaruan penemuan data sensitif otomatis Macie agar temuan cakupan tercermin di semua akun anggota dalam suatu organisasi.

Menekan temuan cakupan

Secara default, temuan cakupan keamanan mengevaluasi fitur Amazon GuardDuty, Amazon Inspector, Amazon Macie, dan AWS Security Hub CSPM mana yang diaktifkan untuk akun dan Wilayah. Jika kemampuan keamanan tertentu tidak berlaku untuk Anda atau merupakan risiko yang diterima, Anda dapat menggunakan fitur penekanan untuk menekan temuan cakupan yang serupa dengan semua temuan lainnya. Ketika temuan cakupan ditekan, itu tidak termasuk dalam perhitungan cakupan dalam widget cakupan keamanan. Widget menampilkan pesan berikut: Cak upan untuk kemampuan keamanan telah dikecualikan melalui temuan cakupan yang ditekan. Pesan tersebut mencakup hitungan temuan yang ditekan.

Untuk menekan temuan cakupan di Hub Keamanan

1. Saat melihat widget cakupan keamanan pilih tautan persen yang tercakup.
2. Dari popup cakupan pilih Lihat temuan cakupan. Setiap temuan dengan status Baru menguraikan kesenjangan cakupan yang diamati.
3. Pilih kotak centang di samping setiap temuan yang ingin Anda tekan.
4. Di bagian atas halaman, pilih Per barui status, lalu pilih Dit ekan.
5. Dalam kotak dialog Setel status ke Ditekan, secara opsional masukkan catatan yang merinci alasan untuk mengubah status. Kemudian pilih Setel status.

Inventaris AI di Security Hub

Inventaris AI di AWS Security Hub memberikan pandangan terpadu tentang sumber daya kecerdasan buatan (AI) dan pembelajaran mesin (ML) Anda di seluruh AWS lingkungan Anda. Gunakan inventaris AI untuk mengidentifikasi beban kerja AI yang tidak disetujui, memahami di mana AI berjalan dan bagaimana itu ditemukan, dan memprioritaskan sumber daya yang memerlukan tinjauan keamanan lebih dekat. Security Hub mengatur sumber daya AI menjadi dua jenis penemuan:

- Dikelola - sumber daya AI yang AWS menyediakan sebagai layanan terkelola. Security Hub menemukan sumber daya ini dari item AWS Config konfigurasi. Jenis sumber daya terkelola mencakup subset Amazon Bedrock, Amazon Bedrock, AgentCore dan Amazon yang didukung. SageMaker
- Self-hostedSumber daya AI yang tidak disediakan sebagai layanan terkelola. Contohnya termasuk model open source, agen, dan server inferensi yang berjalan pada komputasi Anda sendiri. Security Hub mendeteksi sumber daya ini dari sinyal yang berkontribusi pada instans Amazon Elastic Compute Cloud (Amazon EC2) dan image Amazon Elastic Container Registry (Amazon ECR). Sinyal tersebut mencakup temuan tagihan bahan perangkat lunak Amazon Inspector (SBOM) dan aktivitas DNS Amazon GuardDuty .

Akun administrator dapat melihat sumber daya AI dari semua akun yang diaktifkan di organisasinya. Akun anggota hanya dapat melihat sumber daya AI dalam akun mereka sendiri.

Prasyarat untuk penemuan AI yang dihosting sendiri

Penemuan sumber daya AI terkelola tidak memerlukan konfigurasi tambahan selain mengaktifkan Security Hub. Untuk menemukan sumber daya AI yang dihosting sendiri, Anda juga harus mengaktifkan Layanan AWS yang memberikan sinyal yang berkontribusi:

- Amazon Inspector - Aktifkan Amazon Inspector (dengan kebutuhan Security Hub) untuk menghasilkan SBOM. Security Hub menggunakan SBOM ini untuk mendeteksi model yang dihosting sendiri, titik akhir inferensi, dan agen. Untuk instans Amazon EC2, aktifkan pemindaian berbasis agen dengan mode pemindaian yang disempurnakan, pemindaian tanpa agen, atau pemindaian hibrida. Agent-based pemindaian tanpa mode pemindaian yang disempurnakan tidak menghasilkan inventaris perangkat lunak mendalam yang diperlukan oleh deteksi sumber daya AI. Untuk gambar Amazon ECR, Amazon Inspector menyediakan SBOM melalui pemindaian gambar kontainer.

- Amazon GuardDuty — Aktifkan GuardDuty agar Security Hub dapat menggunakan aktivitas DNS untuk mendeteksi titik akhir AI eksternal yang dipanggil instans Amazon EC2 Anda.

Jenis sumber daya AI yang didukung

Pada ketersediaan umum, Security Hub mendukung jenis sumber daya AI yang dihosting sendiri berikut. Security Hub menggunakan sistem deteksi berbasis kepercayaan untuk sumber daya AI yang dihosting sendiri. Setiap deteksi ditambatkan ke sinyal utama, seperti komponen SBOM. Security Hub kemudian menghubungkan sinyal tambahan untuk membangun kepercayaan sebelum sumber daya muncul di inventaris Anda. Security Hub hanya menampilkan sumber daya yang memenuhi ambang kepercayaan, yang membantu meminimalkan positif palsu. Setiap sumber daya menggunakan `SelfHosted::AI::` awalan a. `ResourceType`

- Model (`SelfHosted::AI::Model`) — Model Hugging Face dan Ollama. Security Hub mendeteksi model hanya di direktori model-cache default (seperti cache Hugging Face dan Ollama) dan di jalur khusus yang Anda konfigurasikan untuk pemindaian Amazon Inspector.
- Titik akhir inferensi (`SelfHosted::AI::InferenceEndpoint`) - Perangkat lunak penyajian model yang didukung, seperti VllM, Ollama,, Triton, Text Generation Inference (TGI) TorchServe, SGlang, llama.cpp, LocalAI, BentomL, Xinference, Ray Serve, dan GPT4all.
- Agen (`SelfHosted::AI::Agent`) — OpenClaw agen.
- Titik akhir eksternal (`SelfHosted::AI::ExternalEndpoint`) — Domain layanan AI eksternal yang dipanggil instans Amazon EC2 Anda. Security Hub menyimpan daftar izin domain layanan AI yang dikenal, seperti OpenAI, Anthropic, Cohere, Mistral, dan penyedia AI utama lainnya, dan mendeteksi kapan instans Anda membuat permintaan DNS kepada mereka. Endpoint eksternal terdeteksi dari aktivitas GuardDuty DNS di Amazon EC2 saja.

Sumber daya AI terkelola adalah subset yang didukung dari jenis item SageMaker konfigurasi Amazon Bedrock, Amazon Bedrock, AgentCore dan Amazon, masing-masing dengan kategori sumber daya. `AI/ML`

Menemukan sumber daya AI dari halaman Sumber Daya

Halaman Resources mencantumkan semua sumber daya di lingkungan Anda. Untuk sumber daya AI, Anda dapat menggunakan kemampuan berikut untuk mengidentifikasi beban kerja AI dan host yang menjalankannya:

- AI/ML Sumber daya terkelola menampilkan ikon AI di sebelah sumber daya. Pilih ikon untuk melihat deskripsi.
- Sumber daya host yang menjalankan sumber daya AI yang dihosting sendiri, seperti instans Amazon EC2, menampilkan lencana penghitungan AI yang dihosting sendiri. Host tanpa sumber daya AI yang dihosting sendiri tidak menampilkan lencana.
- Gunakan sakelar filter cepat untuk hanya menampilkan host yang berisi sumber daya AI yang dihosting sendiri.
- Untuk menelusuri host, pilih host untuk membuka panel detailnya, pilih tab aset AI, lalu pilih Lihat semua untuk melihat sumber daya AI yang dihosting sendiri terdeteksi pada host tersebut.

Menggunakan halaman inventaris AI

Halaman inventaris AI berfokus pada sumber daya AI di organisasi Anda. Setiap sumber daya di halaman ini termasuk dalam kategori `AI/ML` sumber daya. Halaman ini menampilkan sumber daya AWS AI terkelola dan sumber daya AI yang dihosting sendiri di lingkungan Anda. Bagian berikut menjelaskan komponen utama halaman.

Bilah ringkasan

Bilah ringkasan menampilkan jumlah total aset AI dan perincian berdasarkan jenis penemuan, baik yang dihosting sendiri atau dikelola. Ini juga menampilkan rincian berdasarkan sub-kategori, seperti model atau agen. Pilih nilai statistik untuk menampilkan detail pendukung dalam tabel.

Pengelompokan, pemfilteran, dan pencarian

Tabel inventaris AI mengelompokkan sumber daya berdasarkan jenis sumber daya secara default. Anda dapat memodifikasi pengelompokan atau menghapusnya untuk mendapatkan tampilan datar semua sumber daya. Bidang pengelompokan yang tersedia mencakup ID kanonik, jenis sumber daya host, tipe penemuan, ID akun, dan jenis sumber daya.

ID kanonik mengidentifikasi apa sumber daya, terlepas dari di mana ia berjalan. Misalnya, dua instans Amazon EC2 yang menjalankan model Hugging Face yang sama berbagi ID kanonik yang sama, sehingga Anda dapat menemukan semua penerapan model tertentu di seluruh organisasi.

> **Note**
>
> ID kanonik dan pengelompokan jenis sumber daya host hanya berlaku untuk sumber daya yang dihosting sendiri. Saat Anda mengelompokkan berdasarkan bidang ini, sumber

daya AI terkelola tidak muncul di hasil karena mereka tidak memiliki atribut ini. Gunakan pengelompokan tipe penemuan atau tipe sumber daya untuk melihat sumber daya terkelola dan yang dihosting sendiri secara bersamaan.

Filter cepat memungkinkan pemfilteran menurut sub-kategori sumber daya atau jenis penemuan. Filter properti mendukung bidang tambahan, termasuk jenis sumber daya host dan ID kanonik untuk sumber daya yang dihosting sendiri.

Detail sumber daya dan sinyal yang berkontribusi

Pilih baris sumber daya untuk membuka panel detail. Untuk sumber daya terkelola, panel menampilkan konfigurasi sumber daya sebagai JSON. Untuk sumber daya yang dihosting sendiri, panel menampilkan sinyal kontribusi yang digunakan Security Hub untuk mendeteksi sumber daya. Sinyal-sinyal ini termasuk sumber deteksi dan detail sinyal individu, seperti komponen SBOM dan perangkat lunak inferensi pendukung untuk model, atau domain DNS untuk titik akhir eksternal.

Bergulir ke sumber daya host

Untuk sumber daya AI yang dihosting sendiri, panel detail menampilkan sumber daya host tempat Security Hub mendeteksi sumber daya. Untuk melihat semua sumber daya AI yang dihosting sendiri pada host yang sama, filter tabel berdasarkan sumber daya host. Dengan tampilan ini, Anda dapat menelusuri dari sumber daya yang dihosting sendiri ke hostnya dan meninjau sumber daya AI yang berdekatan di host tersebut.

Pertimbangan-pertimbangan

Inventaris AI memiliki batasan berikut pada ketersediaan umum:

- Self-hosted Sumber daya AI tidak memiliki temuan dalam rilis ini. Security Hub menunjukkan jumlah pencarian untuk sumber daya AI terkelola saja.
- Self-hosted Deteksi AI didukung pada instans Amazon EC2 dan gambar Amazon ECR saja. AWS Lambda fungsi dan jenis komputasi lainnya tidak didukung.
- Security Hub tidak mengatribusikan image Amazon ECR ke host induk dalam rilis ini, sehingga jumlah AI host tidak menyertakannya.
- Security Hub mendeteksi titik akhir eksternal dari aktivitas GuardDuty DNS di Amazon EC2 saja. Dalam rilis ini, Security Hub tidak mengatribusikan panggilan dari AWS Fargate, AWS Lambda Amazon, SageMaker Amazon EKS, atau komputasi yang dikelola layanan lainnya.

Mengakses inventaris AI dengan API

Anda dapat mengambil data inventaris AI secara terprogram dengan GetResourcesV2 dan operasi. GetResourcesStatisticsV2

Untuk AI/ML sumber daya, `GetResourcesV2` responsnya mencakup `ResourceSubCategory` dan `DiscoveryType` bidang. `DiscoveryType`Bidang menunjukkan apakah sumber daya adalah `Managed` atau`SelfHosted`. Untuk sumber daya AI yang dihosting sendiri dan sumber daya host mereka, responsnya juga disertakan `ResourceInfo` dengan `AIDetails` struktur.

Self-hosted Sumber daya AI menggunakan `SelfHosted::AI::` awalan. `ResourceType` Jenis yang didukung meliputi:

- `SelfHosted::AI::Model`
- `SelfHosted::AI::Agent`
- `SelfHosted::AI::InferenceEndpoint`
- `SelfHosted::AI::ExternalEndpoint`

`AIDetails`Struktur tersebut menghubungkan sumber daya AI yang dihosting sendiri ke hostnya dengan `HostResourceType` bidang `HostResourceGuid` dan. `CanonicalId`Bidang mengidentifikasi sumber daya apa, terlepas dari tempat sumber daya tersebut digunakan, sehingga Anda dapat menggabungkan sumber daya yang identik di beberapa host. ID kanonik menggunakan format: `type/identifier`

- Untuk model ML: `model/<purl>` (misalnya,`model/pkg:huggingface/meta-llama/llama-3-8b`)
- Untuk titik akhir inferensi dan agen: format `type/asset-identifier-name`
- Untuk titik akhir eksternal: domain yang dinormalisasi (misalnya,) `api.*.openai.com`

Pada sumber daya host, seperti instans Amazon EC2, `SelfHostedAI*ResourceCount` bidang dan `SelfHostedTotalAIResourceCount` bidang berisi jumlah sumber daya AI yang dihosting sendiri yang terdeteksi di host.

> **Note**
>
> Saat Anda menggunakan `GetResourcesV2` dan memfilter`ResourceSubCategory`, Anda juga harus menyertakan `ResourceCategory` filter. Atur perbandingan ke `EQUALS` dan

nilainyaAI/ML. Persyaratan ini juga berlaku ketika Anda mengelompokkan berdasarkan ResourceSubCategoryResourceInfo.AIDetails.HostResourceType,, atau ResourceInfo.AIDetails.CanonicalId diGetResourcesStatisticsV2. Jika tidak, operasi mengembalikan aValidationException.
Contoh berikut menunjukkan kombinasi filter yang valid:

```
{
    "Filters": {
        "CompositeFilters": [
            {
                "Operator": "AND",
                "StringFilters": [
                    {
                        "FieldName": "ResourceCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "AI/ML"
                        }
                    },
                    {
                        "FieldName": "ResourceSubCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "Model"
                        }
                    }
                ]
            }
        ]
    }
}
```

Temuan paparan di Security Hub

Penemuan eksposur di Security Hub mewakili korelasi beberapa sinyal keamanan yang mengidentifikasi potensi risiko keamanan di AWS lingkungan Anda. Temuan eksposur membantu Anda memahami dan memprioritaskan risiko keamanan. Mereka secara otomatis menganalisis kombinasi kerentanan, konfigurasi, ancaman, dan hubungan sumber daya. Temuan eksposur mencakup sifat dan sinyal. Sinyal dapat mencakup satu atau lebih jenis sifat eksposur. Security

Hub menghasilkan temuan eksposur ketika sinyal dari Security Hub CSPM, Amazon Inspector, GuardDuty, Macie, atau AWS layanan lain menunjukkan adanya eksposur. Sumber daya dapat menjadi sumber daya utama dalam, paling banyak, satu temuan eksposur. Jika sumber daya tidak memiliki sifat eksposur atau memiliki sifat yang tidak mencukupi, Security Hub tidak menghasilkan temuan eksposur untuk sumber daya tersebut.

Bagaimana temuan eksposur bekerja

Security Hub menghasilkan temuan eksposur dengan:

Menganalisis sinyal dari berbagai layanan AWS keamanan

Security Hub terus mengumpulkan dan menganalisis sinyal keamanan dari beberapa layanan AWS keamanan. Ini menyerap temuan dari GuardDuty untuk deteksi ancaman, Amazon Inspector untuk penilaian kerentanan, Security Hub CSPM untuk pemeriksaan konfigurasi, dan Macie untuk paparan data sensitif. Sinyal-sinyal ini diproses melalui mesin korelasi canggih untuk mengidentifikasi potensi risiko keamanan.

Mengevaluasi konfigurasi sumber daya dan hubungan

Sistem melakukan evaluasi rinci konfigurasi sumber daya terhadap praktik terbaik keamanan. Ini memeriksa pengaturan khusus layanan, persyaratan kepatuhan, dan kontrol keamanan. Analisis ini membantu mengidentifikasi kesalahan konfigurasi yang dapat menyebabkan kerentanan keamanan bila dikombinasikan dengan faktor lain.

Menilai keterjangkauan jaringan

Komponen penting dari temuan eksposur adalah penilaian jangkauan jaringan. Sistem mengevaluasi paparan internet dan jalur akses jaringan internal. Ini menganalisis konfigurasi grup keamanan dan pengaturan ACL jaringan untuk menentukan vektor serangan potensial. Analisis ini membantu mengidentifikasi sumber daya yang mungkin secara tidak sengaja terpapar akses yang tidak sah.

Menghubungkan masalah keamanan terkait

Mesin korelasi memetakan hubungan antara AWS sumber daya, menganalisis bagaimana mereka berinteraksi dan mengidentifikasi potensi implikasi keamanan. Ini memeriksa izin IAM, peran, dan pola akses sumber daya untuk memahami konteks keamanan yang lebih luas. Proses ini membantu mengidentifikasi risiko keamanan yang mungkin ada karena kombinasi konfigurasi individu yang tampaknya tidak bersalah.

Komponen temuan eksposur

Setiap temuan eksposur meliputi:

Judul dan deskripsi potensi risiko keamanan

Setiap temuan eksposur menyertakan judul yang jelas dan deskriptif yang segera menyampaikan sifat risiko keamanan. Deskripsi memberikan informasi terperinci tentang potensi dampak keamanan, sumber daya yang terpengaruh, dan konteks eksposur yang lebih luas. Informasi ini membantu tim keamanan memahami dan menilai risiko dengan cepat.

Klasifikasi tingkat keparahan (Kritis, Tinggi, Sedang, Rendah)

- Tingkat keparahan kritis menunjukkan perhatian segera diperlukan karena kemungkinan eksploitasi yang tinggi dan dampak potensial yang signifikan. Temuan ini biasanya mewakili kerentanan yang mudah ditemukan dan dieksploitasi.
- Tingkat keparahan tinggi menunjukkan perhatian prioritas diperlukan, dengan kemungkinan eksploitasi sedang hingga tinggi dan dampak potensial yang substansif. Temuan ini mungkin relatif mudah dieksploitasi tetapi mungkin memerlukan kondisi tertentu.
- Tingkat keparahan sedang menunjukkan perhatian terjadwal diperlukan, dengan kemungkinan eksploitasi yang lebih rendah dan dampak potensial sedang. Temuan ini biasanya membutuhkan metode eksploitasi yang lebih kompleks.
- Tingkat keparahan rendah menunjukkan perhatian rutin diperlukan, dengan potensi eksploitasi terbatas dan dampak kecil. Temuan ini biasanya sulit untuk dieksploitasi dan menghadirkan risiko minimal.

Sifat yang berkontribusi yang menyebabkan eksposur

Sifat yang berkontribusi mewakili faktor utama yang mengarah pada temuan paparan. Ini termasuk kerentanan keamanan langsung, masalah konfigurasi, kondisi paparan jaringan, dan pengaturan izin sumber daya. Setiap sifat memberikan rincian spesifik tentang bagaimana hal itu berkontribusi terhadap risiko keamanan secara keseluruhan.

Jalur serangan potensial dan visualisasi radius ledakan

Jalur serangan potensial dan visualisasi radius ledakan menyediakan diagram interaktif yang menunjukkan bagaimana penyerang potensial dapat mengeksploitasi paparan yang diidentifikasi. Ini memetakan hubungan sumber daya, jalur jaringan, dan jalur eskalasi hak istimewa ke sumber daya hilir yang berpotensi dapat diakses oleh penyerang jika eksposur dieksploitasi.

Panduan remediasi terperinci

Setiap temuan eksposur mencakup panduan remediasi terperinci dengan langkah-langkah spesifik yang dapat ditindaklanjuti untuk mengatasi risiko yang diidentifikasi. Panduan ini mencakup rekomendasi praktik terbaik, langkah koreksi konfigurasi, dan item tindakan yang diprioritaskan. Panduan ini disesuaikan dengan skenario eksposur spesifik dan mempertimbangkan AWS layanan yang terlibat.

Detail konfigurasi sumber daya

Konfigurasi sumber daya pada saat temuan dibuat serta konfigurasi sumber daya saat ini di dasbor inventaris sumber daya Hub Keamanan.

Sifat kontekstual memberikan konteks keamanan tambahan

Sifat kontekstual adalah penanda keamanan tambahan yang diidentifikasi oleh Security Hub tetapi tidak digunakan untuk membuat temuan eksposur.

Informasi akses yang tidak digunakan dari IAM Access Analyzer dapat muncul sebagai sifat kontekstual dalam temuan eksposur. Ketika peran IAM yang dilampirkan ke sumber daya memiliki izin yang tidak digunakan, Security Hub menyertakan informasi ini sebagai sifat kontekstual dalam tampilan detail eksposur. Misalnya, jika instans Amazon EC2 memiliki kerentanan perangkat lunak dan peran IAM terlampir memiliki 47 izin yang tidak digunakan di 5 layanan, temuan eksposur menunjukkan izin yang tidak digunakan sebagai konteks tambahan. Ini membantu Anda memahami potensi radius ledakan — sumber daya rentan dengan peran IAM yang terlalu istimewa menghadirkan risiko lebih tinggi daripada sumber daya dengan hak istimewa terendah, karena sumber daya yang dikompromikan dapat menggunakan izin yang tidak digunakan tersebut untuk meningkatkan akses.

Jenis sumber daya berikut dapat menampilkan sifat kontekstual akses yang tidak digunakan dalam temuan eksposur mereka:

- Instans Amazon Elastic Compute Cloud
- AWS Lambda fungsi
- Layanan Amazon Elastic Container Service
- Cluster Layanan Amazon Elastic Kubernetes
- Pengguna IAM (langsung)

Klasifikasi tingkat keparahan

Temuan paparan diklasifikasikan berdasarkan:

- Kemudahan penemuan
- Kemudahan eksploitasi
- Kemungkinan eksploitasi
- Kesadaran publik
- Dampak potensial

Untuk informasi selengkapnya, lihat Klasifikasi tingkat keparahan temuan eksposur.

Manfaat temuan eksposur

- Mengurangi analisis manual melalui korelasi otomatis: Temuan eksposur secara signifikan mengurangi waktu dan upaya yang diperlukan untuk analisis keamanan melalui korelasi otomatis dan prioritas risiko cerdas. Security Hub terus memantau AWS lingkungan Anda, secara otomatis mengidentifikasi dan menghubungkan risiko keamanan yang mungkin terlewatkan melalui peninjauan manual.
- Tampilan risiko keamanan yang diprioritaskan: Security Hub menggunakan algoritma penilaian risiko canggih untuk memprioritaskan eksposur berdasarkan tingkat keparahan, dampak, kekritisan sumber daya, dan kemungkinan eksploitasi. Ini membantu tim keamanan memfokuskan upaya mereka pada risiko yang paling signifikan terlebih dahulu, meningkatkan efisiensi operasi keamanan.

Sumber temuan paparan

Temuan eksposur menggabungkan data dari:

- GuardDuty Integrasi Amazon menyediakan kemampuan deteksi ancaman berkelanjutan dalam temuan eksposur. Ini memantau aktivitas berbahaya, potensi kompromi akun, dan anomali perilaku. Sistem menggabungkan temuan ancaman ini ke dalam analisis eksposur yang lebih luas, membantu mengidentifikasi kapan ancaman bergabung dengan masalah keamanan lainnya untuk menciptakan risiko yang signifikan.
- Amazon Inspector menyumbangkan data penilaian kerentanan penting untuk temuan paparan. Ini memberikan informasi terperinci tentang jangkauan jaringan, kerentanan perangkat lunak, dan

pelanggaran praktik terbaik keamanan. Integrasi ini membantu memahami bagaimana kerentanan dapat dieksploitasi melalui jalur serangan yang teridentifikasi.

- AWS Security Hub CSPM memastikan bahwa kepatuhan konfigurasi dan standar keamanan dipertimbangkan dalam analisis eksposur. Ini mengevaluasi sumber daya terhadap kontrol keamanan yang mapan dan praktik terbaik, memberikan dasar untuk memahami risiko berbasis konfigurasi.
- Amazon Macie meningkatkan temuan eksposur dengan kemampuan penemuan dan klasifikasi data sensitif. Ini mengidentifikasi di mana data sensitif ada di AWS lingkungan Anda dan mengevaluasi potensi risiko privasi, membantu memahami dampak potensial dari paparan yang teridentifikasi.

Praktik terbaik

- Tinjau temuan eksposur secara teratur: Manajemen eksposur yang efektif memerlukan proses peninjauan terstruktur. Organisasi harus menerapkan tinjauan harian tentang eksposur kritis, penilaian mingguan status eksposur keseluruhan, analisis tren bulanan, dan evaluasi postur keamanan triwulanan. Pendekatan berlapis ini memastikan perhatian yang tepat terhadap risiko langsung dan tren keamanan jangka panjang.
- Prioritaskan eksposur kritis dan tingkat keparahan tinggi: Manajemen eksposur yang berhasil bergantung pada prioritas risiko yang efektif. Organisasi harus fokus terlebih dahulu pada eksposur kritis sambil mempertimbangkan kekritisan sumber daya dan dampak bisnis. Pendekatan berbasis risiko ini membantu memastikan upaya keamanan selaras dengan prioritas bisnis dan memaksimalkan pengurangan risiko.
- Menerapkan langkah-langkah remediasi yang direkomendasikan: Remediasi paparan harus mengikuti pendekatan sistematis. Organisasi harus dengan hati-hati menerapkan langkah-langkah remediasi yang direkomendasikan, memelihara dokumentasi rinci perubahan, melakukan pengujian modifikasi secara menyeluruh, dan memvalidasi efektivitas perbaikan yang diterapkan. Pendekatan metodis ini membantu memastikan mitigasi risiko yang berhasil sambil menghindari konsekuensi yang tidak diinginkan.
- Konfigurasikan aturan respons otomatis: Memaksimalkan nilai temuan eksposur membutuhkan otomatisasi yang efektif. Organisasi harus menerapkan aturan respons otomatis, mengonfigurasi notifikasi yang sesuai, menetapkan alur kerja yang efisien, dan memelihara jejak audit yang komprehensif. Otomatisasi ini membantu memastikan respons yang konsisten dan tepat waktu terhadap eksposur yang teridentifikasi sekaligus mengurangi upaya manual.

Jenis sumber daya yang didukung untuk temuan eksposur di Hub Keamanan

AWS Security Hub menghasilkan temuan eksposur untuk jenis AWS sumber daya berikut:

- `AWS::DynamoDB::Table`
- `AWS::EC2::Instance`
- `AWS::ECS::Service`
- `AWS::EKS::Cluster`
- `AWS::IAM::User`
- `AWS::Lambda::Function`
- `AWS::RDS::DBInstance`
- `AWS::S3::Bucket`
- `AWS::SageMaker::NotebookInstance`

Jika Anda memiliki konektor Azure, Security Hub juga menghasilkan temuan eksposur untuk jenis sumber daya Azure berikut:

- `microsoft.app/containerapps`
- `microsoft.compute/virtualmachines`
- `microsoft.containerservice/managedclusters`
- `microsoft.documentdb/databaseaccounts`
- `microsoft.graph/user`
- `microsoft.sql/servers/databases`
- `microsoft.storage/storageaccounts/blobservices/containers`
- `microsoft.web/sites`

Security Hub menghasilkan satu temuan eksposur per sumber daya utama. Jika sumber daya tidak memiliki sifat eksposur atau memiliki sifat yang tidak mencukupi, Security Hub tidak menghasilkan temuan eksposur untuk sumber daya tersebut.

Jenis sifat yang didukung di Hub Keamanan

AWS Security Hub menghasilkan temuan eksposur ketika temuan kontrol AWS Security Hub CSPM dan temuan yang dihasilkan oleh dukungan lain Layanan AWS, seperti Amazon Inspector, berisi sifat eksposur untuk sumber daya. Tabel berikut memberikan informasi tentang jenis sifat yang didukung.

Jenis sifat	Deskripsi	Sumber	Sumber daya yang terkena dampak
Asumabilitas	Menunjukkan sumber daya dengan izin yang dijual AWS Identity and Access Management	Konfigurasi sumber daya dari AWS Config	AWS sumber daya dengan AWS Identity and Access Management peran terkait
Dampak	Menunjukkan potensi radius ledakan jika sumber daya dikomprom ikan, berdasarkan izin efektif dari prinsipal AWS Identity and Access Management terkait, termasuk kemampuan untuk membuat dan memodifikasi sumber daya	Analisis izin yang efektif dari prinsipal AWS Identity and Access Management terkait	AWS sumber daya dengan AWS Identity and Access Management identitas terkait
Kesalahan konfigurasi	Menunjukkan sumber daya yang salah konfigurasi	AWS Temuan kontrol CSPM Hub Keamanan, temuan GuardDuty ancaman Amazon, dan informasi tentang konfirmasi sumber daya di. AWS Config	Semua jenis sumber daya

Jenis sifat	Deskripsi	Sumber	Sumber daya yang terkena dampak
Keterjangkauan	Menunjukkan jalur jaringan terbuka ke sumber daya	AWS Temuan kontrol CSPM Security Hub, temuan GuardDuty ancaman Amazon, dan temuan jangkauan jaringan Amazon Inspector.	Instans Amazon EC2, cluster Amazon EKS, fungsi Lambda, dan bucket Amazon S3
Data Sensitif	Menunjukkan bahwa sumber daya berisi data sensitif	Temuan data sensitif Macie	Bucket Amazon S3
Kerentanan	Menunjukkan bahwa sumber daya memiliki kelemahan yang dapat dieksploitasi oleh sumber ancaman.	Temuan kerentanan paket Amazon Inspector dan temuan Malware GuardDuty Amazon Amazon EC2.	Instans Amazon EC2, layanan Amazon ECS, cluster Amazon EKS, dan fungsi Lambda

Setiap sifat dapat dikaitkan dengan beberapa judul yang memberikan detail tentang paparan yang mempengaruhi sumber daya. Misalnya, Anda mungkin melihat judul Exploit Available untuk sifat Ker entanan dalam detail untuk temuan eksposur EC2.

Dampak dan izin efektif

Sifat Impact menggambarkan radius ledakan potensial dari suatu eksposur — sumber daya hilir yang dapat dijangkau dan dikompromikan penyerang jika sumber daya utama dalam temuan

eksposur dikompromikan. Untuk menentukan dampak, Security Hub menganalisis izin efektif dari prinsipal AWS Identity and Access Management (IAM) yang terkait dengan sumber daya.

Izin efektif adalah izin yang sebenarnya dimiliki kepala sekolah setelah Security Hub mengevaluasi kebijakan berbasis identitasnya bersama dengan kebijakan berbasis sumber daya dari sumber daya yang dapat diaksesnya. Karena izin efektif memperhitungkan apa yang diberikan oleh prinsipal dan sumber daya target apa yang diizinkan, izin tersebut lebih akurat mencerminkan tindakan yang dapat dilakukan kepala sekolah daripada kebijakan berbasis identitas saja.

Menggunakan izin yang efektif, Security Hub melacak jalur eskalasi hak istimewa dari sumber daya utama ke sumber daya lain di lingkungan Anda. Setiap jalur adalah rantai sumber daya yang terhubung oleh izin yang memungkinkan penyerang untuk berpindah dari satu sumber daya ke sumber daya berikutnya. Saat Security Hub mengidentifikasi jalur konkret ke sumber daya yang ada, jalur tersebut akan muncul sebagai bagian dari sifat D ampak. Impact juga memperhitungkan izin di luar jalur ini, seperti kemampuan untuk memanggil Layanan AWS yang dapat membuat atau memodifikasi sumber daya lain. Anda dapat meninjau jalur ini di grafik jalur serangan potensial dan mengurangi radius ledakan Anda dengan menghapus izin yang tidak perlu. Untuk informasi selengkapnya, lihat Melihat eksposur di Security Hub dengan grafik jalur serangan potensial.

Menghasilkan temuan eksposur

Security Hub menghasilkan temuan eksposur hampir secara real-time. Saat temuan keamanan baru dicerna dan temuan yang ada diperbarui, Security Hub menghasilkan atau memperbarui temuan eksposur hampir secara real time. Security Hub menghasilkan satu temuan eksposur per ID sumber daya.

Security Hub tidak mempublikasikan temuan eksposur untuk jenis sumber daya yang tidak didukung oleh temuan eksposur. Ketika sumber daya memiliki jumlah dan kombinasi sifat yang signifikan, Security Hub menghasilkan temuan eksposur. Jumlah dan kombinasi sifat juga menentukan tingkat keparahan temuan paparan.

Temuan eksposur sampel

AWS Security Hub menormalkan temuan eksposur di Open Cybersecurity Schema Framework (OCSF).

Temuan eksposur sampel

Dalam contoh temuan paparan berikut, `related_events` parameter berisi detail unik untuk temuan eksposur, seperti temuan yang berkontribusi. Temuan yang berkontribusi adalah sifat dan sinyal

yang terkait dengan temuan eksposur. Satu temuan yang berkontribusi dapat mencakup satu atau lebih sifat. `observables`Parameter mengidentifikasi sumber daya yang terkait dengan temuan yang berkontribusi. Ini bisa berbeda dari `resources` parameter, yang mengidentifikasi sumber daya yang terkait dengan temuan eksposur.


```
{
    "activity_id": 1,
    "activity_name": "Create",
    "category_name": "Findings",
    "category_uid": 2,
    "class_name": "Detection Finding",
    "class_uid": 2004,
    "cloud": {
        "account": {
            "uid": "123456789012",
            "name": "production-application"
        },
        "cloud_partition": "aws",
        "provider": "AWS",
        "region": "us-east-1"
    },
    "finding_info": {
        "analytic": {
            "name": "Exposure",
            "type": "Rule",
            "type_id": 1,
            "uid": "0.0.1"
        },
        "created_time_dt": "2024-11-15T21:39:26.337224100Z",
        "desc": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "finding.info.modified_time_dt": "2024-11-15T21:39:26.337224100Z",
        "related_events_count": 3,
        "related_events": [
            {
                "tags": [
                    {
                        "name": "Vulnerability",
                        "values": [
                            "Attack Vector Network",
                            "EPSS Level >= High",
                            "EPSS Level >= Medium",
                            "Exploit Available",
```

```
                            "No Privileges Required",
                            "No User Interaction Required",
                            "Vulnerable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/inspector"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "CVE-2023-33246 - org.apache.rocketmq:rocketmq-controller",
                "uid": "arn:aws:inspector2:us-
east-1:123456789012:finding/1234567890abcdef0"
            },
            {
                "tags": [
                    {
                        "name": "Reachability",
                        "values": [
                            "Publicly Invocable"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title":  "Lambda function policies should prohibit public access",
```

```
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa"
            },
            {
                "tags": [
                    {
                        "name": "Misconfiguration",
                        "values": [
                            "Deployed outside VPC"
                        ]
                    }
                ],
                "product": {
                    "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub"
                },
                "observables": [
                    {
                        "type": "Resource UID",
                        "type_id": 10,
                        "value": "arn:aws:lambda:us-east-1:123456789012:application-
function"
                    }
                ],
                "type": "Finding",
                "title": "Lambda functions should be in a VPC",
                "uid": "arn:aws:securityhub:us-east-1:123456789012:security-control/
Lambda.3/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            }
        ],
        "title": "Publicly invocable Lambda function executed outside of VPC has
 vulnerability with known exploit that can be exploited from remote network",
        "types": [
            "Exposure/Potential Impact/Resource Hijacking"
        ],
        "uid": "arn:aws:securityhub:us-
east-1:123456789012:risk:1234f781c7ae7507f01e2fb460f15ca8fe7f9c95e257698a092cb74a4ea84a42"
    },
    "metadata": {
        "product": {
            "name": "Security Hub Exposure Analysis",
            "uid": "arn:aws:securityhub:us-east-1::productv2/aws/securityhub-risk",
            "vendor_name": "Amazon"
        },
        "processed_time_dt": "2024-11-15T21:39:58.819Z",
```

```
        "profiles": [
            "cloud",
            "datetime"
        ],
        "version": "1.4.0-dev"
    },
    "resources": [
        {
            "cloud_partition": "aws",
            "region": "us-east-1",
            "tags": [
                {
                    "name": "aws:cloudformation:stack-name",
                    "value": "LambdaProdStack"
                },
                {
                    "name": "aws:cloudformation:stack-id",
                    "value": "arn:aws:cloudformation:us-east-1:123456789012:stack/
LambdaProdStack/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222"
                },
                {
                    "name": "aws:cloudformation:logical-id",
                    "value": "lambdar3function94D10D40"
                }
            ],
            "type": "AwsLambdaFunction",
            "uid": "arn:aws:lambda:us-east-1:123456789012:application-function"
        }
    ],
    "severity": "Critical",
    "severity_id": 5,
    "impact": "High",
    "impact_id": 3,
    "likelihood": "Very High",
    "likelihood_id": 5,
    "status": "New",
    "status_id": 1,
    "time": 1731706766337,
    "time_dt": "2024-11-15T21:39:26.337224100Z",
    "type_name": "Detection Finding: Create",
    "type_uid": 200401,
    "vendor_attributes": {
        "severity_id": 5,
        "severity": "Critical"
```

```
    }
}
```

Menentukan tingkat keparahan temuan eksposur

AWS Security Hub menetapkan setiap eksposur untuk menemukan tingkat keparahan default`CRITICAL`,`HIGH`,`MEDIUM`, atau`LOW`. Temuan paparan dengan tingkat keparahan tidak `INFORMATIONAL` dipublikasikan. Security Hub menentukan tingkat keparahan temuan eksposur dengan menggabungkan dua dimensi, kemungkinan dan dampak, pada matriks risiko. Kemungkinan mencerminkan seberapa mudah eksposur dapat dieksploitasi, dan dampak mencerminkan besarnya kerugian jika dieksploitasi.

Dalam kasus di mana dampak tidak dapat ditentukan untuk sumber daya, tingkat keparahan didasarkan murni pada kemungkinan.

Matriks risiko

Tabel berikut menunjukkan bagaimana kemungkinan dan dampak bergabung untuk menghasilkan tingkat keparahan akhir dari temuan eksposur. Kemungkinan menetapkan tingkat keparahan dasar, dan dampak menyesuaikannya: dampak tinggi meningkatkan tingkat keparahan satu tingkat (dibatasi pada`CRITICAL`), dampak sedang membuat tingkat keparahan tidak berubah, dan dampak rendah mengurangi tingkat keparahan satu tingkat (di `INFORMATIONAL` lantai). Dampak hanya menyesuaikan tingkat keparahan yang ditetapkan kemungkinan. Dampak saja tidak menghasilkan temuan eksposur.

Matriks risiko keparahan

Kemungkinan ↓/Dampak →	Rendah	Sedang	Tinggi
Sangat Tinggi	TINGGI	KRITIS	KRITIS
Tinggi	SEDANG	TINGGI	KRITIS
Sedang	RENDAH	SEDANG	TINGGI
Rendah	INFORMASI	RENDAH	SEDANG

> **Note**
>
> Kemungkinan rendah dikombinasikan dengan dampak rendah menghasilkan tingkat keparahan`INFORMATIONAL`. Security Hub tidak mempublikasikan temuan eksposur dengan tingkat keparahan ini, sehingga tidak muncul di halaman Eksposur atau dalam GetFindingsV2 hasil.

Kemungkinan

Kemungkinan mengukur seberapa mudah eksposur dapat dieksploitasi, berdasarkan sifat-sifat berkontribusi yang ada pada sumber daya, seperti Asumabilitas, Kesalahan Konfigurasi, Jangkauan, Data Sen sitif, dan Ker entanan. Security Hub menggunakan beberapa karakteristik untuk menilai kemungkinan, termasuk yang berikut:

- Kesadaran — Sejauh mana paparan tidak teoretis, tetapi memiliki eksploitasi yang tersedia untuk umum atau otomatis.
- Kemudahan penemuan — Apakah alat otomatis, seperti pemindaian port atau pencarian internet, tersedia untuk menemukan sumber daya yang berisiko.
- Kemudahan eksploitasi — Kemudahan di mana aktor ancaman dapat mengeksploitasi eksposur. Misalnya, jika jalur jaringan terbuka atau metadata yang salah konfigurasi ada, aktor ancaman dapat lebih mudah mengeksploitasi eksposur.
- Kemungkinan eksploitasi — Kemungkinan eksposur akan dieksploitasi dalam 30 hari ke depan. Faktor ini sesuai dengan Sistem Penilaian Prediksi Eksploit (EPSS).

Dampak

D ampak mengukur besarnya kerusakan lingkungan Anda jika paparan dieksploitasi. Misalnya, paparan dapat menyebabkan hilangnya akuntabilitas, hilangnya ketersediaan, hilangnya kerahasiaan dari paparan data, atau hilangnya integritas dari korupsi data.

Untuk menilai dampak, Security Hub menganalisis izin efektif dari prinsipal yang AWS Identity and Access Management terkait dengan sumber daya untuk menentukan tindakan yang dapat dipanggil Layanan AWS oleh penyerang. Ini juga mengidentifikasi sumber daya yang ada yang dapat dicapai penyerang dan kompromi melalui eskalasi hak istimewa. Untuk informasi selengkapnya, lihat Dampak dan izin efektif.

Meninjau temuan eksposur

Anda dapat meninjau semua temuan eksposur Anda di konsol Hub Keamanan dan dengan GetFindingsV2 API. Halaman Eksposur di konsol Hub Keamanan menampilkan semua temuan eksposur aktif. Temuan paparan terdaftar dengan penurunan tingkat keparahan. Anda dapat memfilter temuan eksposur dengan menambahkan dan menghapus filter dengan bilah pencarian Tambah filter. Anda dapat mengelompokkan temuan eksposur Anda dengan Grup berdasarkan dropdown. Anda juga dapat memfilter temuan eksposur dengan menu Filter cepat.

Rincian untuk temuan eksposur

Anda dapat melihat banyak detail untuk temuan eksposur. Rincian ini dibagi di antara tab di konsol Hub Keamanan. Tab I khtisar memberikan detail utama tentang temuan eksposur. Tab S ifat mencantumkan sifat dan sinyal yang terkait dengan temuan eksposur. Tab Resources menyediakan detail tentang tag sumber daya dan sumber daya yang terkait dengan temuan eksposur. Daftar berikut memberikan deskripsi untuk detail pencarian eksposur.

- Judul pencarian — Judul temuan eksposur.
- Tingkat keparahan — Tingkat keparahan temuan paparan. Security Hub menggunakan jumlah dan kombinasi sifat untuk sumber daya untuk menentukan tingkat keparahan temuan eksposur. Tingkat keparahan bisa`CRITICAL`,`HIGH`,`MEDIUM`, atau`LOW`. Security Hub tidak mempublikasikan temuan eksposur dengan tingkat keparahan`INFORMATIONAL`. Anda dapat memperbarui `Severity` melalui konsol Hub Keamanan atau dengan operasi BatchUpdateFindingsV2 API.
- Deskripsi — Deskripsi temuan eksposur.
- Jenis — Nama jenis pencarian eksposur. Misalnya, namanya mungkin menyerupai`Exposure/ Potential Impact/Resource Hijacking`.
- Akun — ID Akun AWS tempat temuan eksposur dihasilkan.
- Usia — Menunjukkan berapa lama temuan paparan telah aktif.
- Waktu yang dibuat — Stempel waktu yang menunjukkan kapan temuan eksposur dibuat.
- Waktu yang dimodifikasi — Stempel waktu yang menunjukkan kapan temuan eksposur terakhir diperbarui.
- Wilayah — Wilayah AWS Tempat temuan eksposur dihasilkan.
- Nama produk — Nama produk yang menghasilkan temuan eksposur. Ini akan selalu menjadi Deteksi Eksposur Hub Keamanan.
- Nama perusahaan — Nama perusahaan yang menghasilkan temuan eksposur. Ini akan selalu terjadi AWS.

- Nama aktivitas — Nama aktivitas yang terakhir dilakukan terhadap temuan.
- Status — Status temuan eksposur ini.
- ID Penem uan — Pengidentifikasi unik yang terkait dengan temuan eksposur.
- Jalur serangan potensial (hanya konsol) — Visualisasi interaktif yang menunjukkan bagaimana penyerang potensial dapat mengakses dan mengendalikan sumber daya yang terkait dengan temuan eksposur. Untuk informasi selengkapnya, lihat Melihat eksposur di Security Hub dengan grafik jalur serangan potensial.
- Sifat — Mengidentifikasi jenis sifat dan judul sifat yang terkait dengan temuan paparan. Di konsol Hub Keamanan, Anda dapat melihat sifat berdasarkan jenis sifat atau sinyal. Ini membantu Anda menganalisis temuan yang berkontribusi dalam konteks paparan terkait.
- Remediasi — Tautan ke dokumentasi remediasi khusus untuk sifat-sifat yang diidentifikasi dalam paparan.
- Sumber Daya — Mengidentifikasi sumber daya yang terkait dengan temuan eksposur.

Meninjau detail untuk temuan eksposur

Topik ini menjelaskan cara meninjau detail tentang temuan ekspo AWS sur di konsol Hub Keamanan dan dengan API.

Meninjau detail untuk temuan eksposur di konsol Hub Keamanan

Untuk melihat detail untuk temuan eksposur di konsol Hub Keamanan

1. Masuk menggunakan kredensional Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Ek sposur.
3. Pilih temuan eksposur yang ingin Anda lihat detailnya.

Meninjau detail untuk temuan eksposur dengan API

Anda dapat meninjau temuan ekspo GetFindingsV2 sur dengan API atau dengan AWS CLI. Anda dapat memfilter semua temuan ekspo `metadata.product.feature.uid` sur dengan bidang dengan `security-hub/Exposure` nilai. Untuk informasi selengkapnya, lihat GetFindingsV2.

Perintah contoh

Berikut ini adalah AWS CLI contoh yang mengambil 10 temuan eksposur terbaru yang dihasilkan di akun Anda. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
aws securityhub get-findings-v2 \
--max-results '10' \
--filter '{"CompositeFilters": [{"StringFilters":
 [{"FieldName":"metadata.product.feature.uid","Filter": {"Value":"security-hub/
Exposure","Comparison":"EQUALS"}} ]}]}'
```

Melihat eksposur di Security Hub dengan grafik jalur serangan potensial

Grafik jalur serangan potensial adalah visualisasi interaktif yang menunjukkan bagaimana penyerang potensial dapat mengakses dan mengendalikan sumber daya yang terkait dengan temuan eksposur. Anda dapat mengakses grafik ini hanya di konsol Hub Keamanan dari halaman Ek sposur. Saat Anda melihat detail untuk temuan eksposur, tab I khtisar menyertakan bagian yang disebut Jalur serangan potensial dan radius ledakan.

Grafik jalur serangan menunjukkan sumber daya utama tempat eksposur dihasilkan, jalur jaringan (jika ada), dan sumber daya hilir yang dapat dijangkau penyerang dengan meningkatkan izin. Ketika Security Hub mengidentifikasi jalur eskalasi hak istimewa konkret dari sumber daya utama ke sumber daya lain di lingkungan Anda, itu menampilkannya sebagai bagian radius ledakan dari grafik. Setiap node mewakili sumber daya, dan koneksi antar node menunjukkan izin yang memungkinkan penyerang untuk berpindah dari satu sumber daya ke sumber daya berikutnya.

Di bagian tab Ikhtis ar ini, Anda dapat memilih dan menyeret AWS sumber daya di grafik jalur serangan potensial. Anda dapat fokus pada area tertentu dari grafik jalur serangan dengan ikon zoom-in dan zoom-out. Anda dapat memperluas grafik jalur serangan masuk dan keluar dari mode layar penuh melalui ikon layar penuh. Legenda mengkode sumber daya utama, sumber daya yang terlibat, sumber daya radius ledakan, dan jumlah sifat yang berkontribusi berdasarkan warna dan menunjukkan kategori sifat dan jumlah sifat dalam grafik jalur serangan. Anda dapat melihat detail untuk sumber daya dengan memilih sumber daya dan memilih Lihat detail sumber daya. Anda juga dapat menyalin ID dan Akun AWS nomor yang terkait dengan sumber daya. Temuan paparan dengan sifat jangkauan menunjukkan internet publik dan jalur jaringan yang runtuh dalam grafik jalur serangan. Anda dapat melihat detail ini dengan memilih simpul jalur jaringan yang runtuh.

Untuk melihat sumber daya hilir dan jalur eskalasi hak istimewa yang menghubungkannya, pilih tab Penilaian dampak. Setiap jalur menunjukkan rantai sumber daya yang dapat dilalui penyerang dan

izin spesifik pada setiap langkah. Untuk informasi selengkapnya tentang sifat dampak dan izin efektif, lihatDampak dan izin efektif.

Memperbaiki temuan paparan

Topik di bagian ini menjelaskan langkah-langkah remediasi untuk temuan paparan di berbagai Layanan AWS hal.

Bid `Remediation` ang format OCSF berisi dua bidang: `remediation` dan`references`.

```
"Remediation": {
    "Recommendation": {
        "remediation":{"desc":"String",
        "references":["string array"]}
    }
},
```

> **Note**
>
> Panduan remediasi yang diberikan di bagian berikut mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Memperbaiki eksposur untuk tabel DynamoDB

AWS Security Hub dapat menghasilkan temuan eksposur untuk tabel DynamoDB.

Pada konsol Hub Keamanan, tabel DynamoDB yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber Daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan

menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat salah konfigurasi di DynamoDB
  - Tabel DynamoDB menonaktifkan pemulihan point-in-time
  - Tabel DynamoDB tidak tercakup oleh rencana cadangan
  - Tabel DynamoDB memiliki perlindungan penghapusan dinonaktifkan

Sifat salah konfigurasi di DynamoDB

Berikut ini menjelaskan sifat kesalahan konfigurasi dan langkah-langkah remediasi untuk tabel DynamoDB.

Tabel DynamoDB menonaktifkan pemulihan point-in-time

Remediasi: Aktifkan pemulihan point-in-time DynamoDB

Pemulihan point-in-time DynamoDB menyediakan pencadangan otomatis berkelanjutan untuk data tabel DynamoDB Anda. Untuk informasi tentang cara mengembalikan tabel DynamoDB ke titik waktu tertentu, lihat Memulihkan tabel DynamoDB ke titik waktu di Panduan Pengembang Amazon DynamoDB.

Tabel DynamoDB tidak tercakup oleh rencana cadangan

AWS Backup menyediakan layanan terpusat untuk mengkonfigurasi, mengelola, dan mengotomatiskan pencadangan di seluruh AWS layanan, termasuk DynamoDB. Tanpa rencana cadangan, tabel Anda tidak memiliki pencadangan otomatis terjadwal dengan periode retensi yang dapat disesuaikan, menciptakan risiko keamanan yang signifikan. Penyerang dapat merusak atau menghapus data tabel Anda dengan jahat. Tanpa pencadangan yang tepat, Anda mungkin tidak memiliki opsi pemulihan di luar jendela Pem Point-in-Time ulihan (jika diaktifkan), berpotensi

mengakibatkan hilangnya data permanen. Mengikuti praktik terbaik perlindungan data, tutupi tabel DynamoDB Anda dengan paket cadangan.

Remediasi: Buat rencana cadangan

Sebelum membuat rencana cadangan, tentukan frekuensi pencadangan dan periode retensi yang sesuai untuk data Anda. Untuk informasi tentang cara membuat rencana cadangan, lihat Men etapkan sumber daya ke rencana cadangan di Panduan Pengembang Cadangan. AWS

Tabel DynamoDB memiliki perlindungan penghapusan dinonaktifkan

Perlindungan penghapusan mencegah penghapusan tabel DynamoDB secara tidak sengaja. Saat perlindungan penghapusan dinonaktifkan, tabel DynamoDB rentan terhadap penghapusan yang tidak diinginkan melalui tindakan konsol, panggilan API, perintah CLI, atau proses otomatis. Hal ini dapat mengekspos AWS lingkungan Anda terhadap kehilangan data, karena entitas yang tidak sah dengan akses ke AWS lingkungan Anda dapat dengan sengaja menghapus tabel, mengakibatkan gangguan layanan dan kehilangan data permanen. Mengikuti praktik terbaik perlindungan data, aktifkan perlindungan data untuk tabel DynamoDB.

Remediasi: Aktifkan perlindungan penghapusan

Jika Anda mengelola beberapa tabel, pertimbangkan CloudFormation untuk menggunakan untuk memperbarui properti tabel secara massal. Anda dapat memodifikasi CloudFormation template Anda untuk menyertakan `DeletionProtectionEnabled` properti dan memperbarui tumpukan Anda. Setelah menyelesaikan remediasi, verifikasi perlindungan penghapusan diaktifkan di dropdown Info tambahan di tab Peng aturan tabel.

Memperbaiki eksposur untuk instans EC2

AWS Security Hub dapat menghasilkan temuan eksposur untuk instans Amazon Elastic Compute Cloud (EC2).

Pada konsol Hub Keamanan, instans EC2 yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber Daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak

penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat kesalahan konfigurasi untuk instans EC2
  - Instans EC2 memungkinkan akses ke IMDS menggunakan versi 1
  - Instans Amazon EC2 memiliki grup keamanan atau ACL jaringan yang memungkinkan akses SSH atau RDP
  - Instans Amazon EC2 memiliki grup keamanan terbuka
- Sifat jangkauan untuk instans EC2
  - Instans EC2 dapat dijangkau melalui internet
- Ciri-ciri kerentanan untuk instans EC2
  - Instans EC2 memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi
  - Instans Amazon EC2 memiliki kerentanan perangkat lunak
  - Instans EC2 memiliki sistem End-Of-Life operasi
  - Instans EC2 memiliki paket perangkat lunak berbahaya
  - Instans EC2 memiliki file berbahaya
- Sifat dampak untuk instans EC2
  - Memiliki jalur eksekutor istimewa kontrol penuh
  - Memiliki jalur eskalasi kebijakan langsung
  - Memiliki jalur pembajakan kebijakan kepercayaan

- Memiliki jalur data ransomware
- Telah menghapus jalur pembatasan
- Memiliki jalur pass role buat eksekutor
- Memiliki jalur pelaksana peran swap yang ada
- Memiliki jalur eskalasi rantai peran
- Telah menyuntikkan jalur eksekutor istimewa kode
- Telah menonaktifkan jalur jejak audit
- Memiliki akses jalur eksekutor yang ada
- Memiliki jalur pencetakan kredensi
- Memiliki jalur akses data peran pass
- Memiliki jalur pembajakan tugas peran lulus
- Memiliki jalur akses data hop tunggal
- Memiliki jalur kemajuan kemampuan

Sifat kesalahan konfigurasi untuk instans EC2

Berikut adalah sifat kesalahan konfigurasi untuk instans EC2 dan langkah-langkah remediasi yang disarankan.

Instans EC2 memungkinkan akses ke IMDS menggunakan versi 1

Metadata instans adalah data tentang instans Amazon EC2 yang dapat digunakan aplikasi untuk mengonfigurasi atau mengelola instans yang sedang berjalan. Layanan metadata instans (IMDS) adalah komponen pada instans yang menggunakan kode pada instans untuk mengakses metadata instans dengan aman. Jika IMDS tidak diamankan dengan benar, IMDS dapat menjadi vektor serangan potensial, karena memberikan akses ke kredenSIAL sementara dan data konfigurasi sensitif lainnya. IMDSv2 memberikan perlindungan yang lebih kuat terhadap eksploitasi melalui otentikasi berorientasi sesi, membutuhkan token sesi untuk permintaan metadata dan membatasi durasi sesi. Mengikuti prinsip keamanan standar, konfigurasikan instans Amazon EC2 untuk menggunakan IMDSv2 dan menonaktifkan IMDSv1.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Uji kompatibilitas aplikasi

Sebelum menerapkan IMDSv2, uji instans Anda untuk memastikan kompatibilitasnya dengan IMDSv2. Beberapa aplikasi atau skrip mungkin memerlukan IMDSv1 untuk fungsionalitas inti dan memerlukan konfigurasi tambahan. Untuk informasi selengkapnya tentang alat dan jalur yang direkomendasikan untuk menguji kompatibilitas aplikasi, Trans isi ke menggunakan Layanan Metadata Instance Versi 2 di Panduan Pengguna Amazon Elastic Compute Cloud.

Perbarui instance untuk menggunakan IMDSv2

Ubah instans yang ada untuk menggunakan IMDSv2. Untuk informasi selengkapnya, lihat Mengubah opsi metadata instans untuk instans yang ada di Panduan Pengguna Amazon Elastic Compute Cloud.

Menerapkan pembaruan ke instans dalam grup Penskalaan Otomatis

Jika instance Anda adalah bagian dari grup Penskalaan Otomatis, perbarui template peluncuran atau konfigurasi luncurkan Anda dengan konfigurasi baru, dan lakukan penyegaran instance.

Instans Amazon EC2 memiliki grup keamanan atau ACL jaringan yang memungkinkan akses SSH atau RDP

Protokol akses jarak jauh seperti SSH dan RDP memungkinkan pengguna untuk terhubung ke dan mengelola instans Amazon EC2 dari lokasi eksternal. Ketika grup keamanan mengizinkan akses tak terbatas ke protokol ini dari internet, mereka meningkatkan permukaan serangan instans Amazon EC2 Anda dengan mengizinkan akses internet ke instans Anda. Mengikuti prinsip-prinsip keamanan standar, batasi akses jarak jauh ke alamat atau rentang IP tertentu yang tepercaya.

Remediasi: Ubah aturan grup keamanan

Batasi akses ke instans Amazon EC2 Anda ke alamat IP tepercaya tertentu. Batasi akses SSH dan RDP ke alamat IP tepercaya tertentu, atau gunakan notasi CIDR untuk menentukan rentang IP (misalnya, 192.168.1. 0/24). Untuk mengubah aturan grup keamanan, lihat Meng onfigurasi aturan grup keamanan di Panduan Pengguna Amazon Elastic Compute Cloud.

Instans Amazon EC2 memiliki grup keamanan terbuka

Grup keamanan bertindak sebagai firewall virtual untuk instans Amazon EC2 Anda untuk mengontrol lalu lintas masuk dan keluar. Grup keamanan terbuka, yang memungkinkan akses tidak terbatas dari alamat IP apa pun, dapat mengekspos instans Anda ke akses yang tidak sah. Mengikuti prinsip keamanan standar, batasi akses grup keamanan ke alamat IP dan port tertentu.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau aturan grup keamanan dan menilai konfigurasi saat ini

Evaluasi port mana yang terbuka dan dapat diakses dari rentang IP yang luas, seperti(`0.0.0.0/0` or `::/0`). Untuk petunjuk tentang melihat detail grup keamanan, lihat DescribeSecurityGroups di Porting Assistant for .NET API Reference.

Ubah aturan grup keamanan

Ubah aturan grup keamanan Anda untuk membatasi akses ke alamat atau rentang IP tepercaya tertentu. Saat memperbarui aturan grup keamanan Anda, pertimbangkan untuk memisahkan persyaratan akses untuk segmen jaringan yang berbeda dengan membuat aturan untuk setiap rentang IP sumber yang diperlukan atau membatasi akses ke port tertentu. Untuk mengubah aturan grup keamanan, lihat Meng onfigurasi aturan grup keamanan di Panduan Pengguna Amazon EC2.

Sifat jangkauan untuk instans EC2

Berikut adalah ciri-ciri jangkauan untuk instans EC2 dan langkah-langkah remediasi yang disarankan.

Instans EC2 dapat dijangkau melalui internet

Instans Amazon EC2 dengan port yang dapat dijangkau dari internet dapat mengekspos instans Anda. Jangkauan dapat terjadi melalui gateway internet (termasuk contoh di belakang Application Load Balancers atau Classic Load Balancers), koneksi peering VPC, atau gateway virtual VPN. Mengikuti prinsip-prinsip keamanan standar, terapkan kontrol akses jaringan dengan hak istimewa terendah dengan membatasi lalu lintas masuk hanya ke sumber dan port yang diperlukan.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Memodifikasi atau hapus aturan grup keamanan

Di tab Sumber Daya, buka sumber daya untuk Grup Keamanan Amazon EC2. Tinjau apakah akses internet diperlukan agar instance berfungsi. Ubah atau hapus aturan grup keamanan masuk yang mengizinkan akses tidak terbatas (`0.0.0.0/0`atau`::/0`). Menerapkan aturan yang lebih ketat berdasarkan rentang IP atau grup keamanan tertentu. Jika akses publik terbatas diperlukan, batasi akses ke port dan protokol tertentu yang diperlukan untuk fungsi instance. Untuk petunjuk

tentang mengelola aturan grup keamanan, lihat Meng onfigurasi aturan grup keamanan di Panduan Pengguna Amazon EC2.

Perbarui ACL jaringan

Meninjau dan memodifikasi daftar kontrol akses jaringan (ACL) yang terkait dengan subnet instance. Pastikan pengaturan ACL selaras dengan perubahan grup keamanan dan jangan secara tidak sengaja mengizinkan akses publik. Untuk petunjuk tentang memodifikasi ACL jaringan, lihat Bekerja dengan ACL jaringan di Panduan Pengguna Amazon VPC.

Metode akses alternatif

Pertimbangkan opsi berikut untuk metode akses alternatif:

- Gunakan NAT Gateway untuk konektivitas internet keluar — Untuk instance di subnet pribadi yang memerlukan akses ke internet (misalnya, untuk mengunduh pembaruan), pertimbangkan untuk menggunakan NAT Gateway alih-alih menetapkan alamat IP publik. NAT Gateway memungkinkan instans di subnet pribadi untuk memulai koneksi keluar ke internet sambil mencegah koneksi masuk dari internet.
- Gunakan Manajer Sesi Sistem - Manajer Sesi menyediakan akses shell yang aman ke instans Amazon EC2 Anda tanpa perlu port masuk, mengelola kunci SSH, atau memelihara host bastion.
- Gunakan WAF dan Elastic Load Balancing atau Application Load Balancer — Untuk instans yang menjalankan aplikasi web, pertimbangkan untuk menggunakan LB yang dikombinasikan dengan AWS Web Application Firewall (WAF). LB dapat dikonfigurasi untuk memungkinkan instans Anda berjalan di subnet pribadi sementara LB berjalan di subnet publik dan menangani lalu lintas internet. Menambahkan WAF ke penyeimbang beban Anda memberikan perlindungan tambahan terhadap eksploitasi web dan bot.

Ciri-ciri kerentanan untuk instans EC2

Berikut adalah ciri-ciri kerentanan untuk instans EC2 dan langkah-langkah remediasi yang disarankan.

Instans EC2 memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

Paket perangkat lunak yang diinstal pada instans EC2 dapat terkena Kerentanan dan Eksposur Umum (CVE). CVE kritis menimbulkan risiko keamanan yang signifikan bagi AWS lingkungan Anda. Prinsipal yang tidak sah dapat mengeksploitasi kerentanan yang tidak ditambal ini untuk

membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Kerentanan kritis dengan kemungkinan eksploitasi tinggi mewakili ancaman keamanan langsung, karena kode eksploitasi mungkin sudah tersedia untuk umum dan secara aktif digunakan oleh penyerang atau alat pemindaian otomatis. Tambal kerentanan ini untuk melindungi instans Anda.

Remediasi: Perbarui instans yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan pada sifat tersebut. Dokumentasi vendor mungkin mencakup panduan remediasi khusus. Ikuti remediasi yang sesuai menggunakan pedoman umum ini:

Gunakan System Manager Patch Manager untuk menerapkan patch untuk sistem operasi dan aplikasi. Patch Manager membantu Anda memilih dan menerapkan sistem operasi dan patch perangkat lunak secara otomatis pada kelompok instans yang besar. Jika Patch Manager tidak dikonfigurasi, perbarui sistem operasi secara manual pada setiap instans yang terpengaruh.

Perbarui aplikasi yang terpengaruh ke versi aman terbaru mengikuti prosedur yang direkomendasikan vendor. Untuk mengelola pembaruan aplikasi di beberapa instans, pertimbangkan untuk menggunakan Manajer Status Manajer Sistem untuk menjaga perangkat lunak Anda dalam keadaan yang konsisten. Jika pembaruan tidak tersedia, pertimbangkan untuk menghapus atau menonaktifkan aplikasi rentan sampai patch dirilis atau mitigasi lainnya, seperti membatasi akses jaringan ke aplikasi atau menonaktifkan fitur rentan.

Ikuti saran remediasi khusus yang diberikan dalam temuan Inspektur Amazon. Ini bisa melibatkan perubahan aturan grup keamanan, memodifikasi konfigurasi instance, atau menyesuaikan pengaturan aplikasi.

Periksa apakah instance tersebut merupakan bagian dari Grup Penskalaan Otomatis. AMI-replacement tambalan dilakukan pada infrastruktur yang tidak dapat diubah dengan memperbarui ID AMI yang dikonfigurasi untuk menerapkan instans Amazon EC2 baru dalam grup Penskalaan Otomatis. Jika Anda menggunakan custom/golden AMI, buat instance dengan AMI baru, lalu sesuaikan instance dan buat AMI emas baru Untuk informasi selengkapnya, lihat tambalan pembaruan AMI (menggunakan AMI yang ditambal untuk grup Penskalaan Otomatis).

Pertimbangan masa depan

Untuk mencegah kejadian di masa mendatang, pertimbangkan untuk menerapkan program manajemen kerentanan. Amazon Inspector dapat dikonfigurasi untuk secara otomatis memindai CVE pada instans Anda. Amazon Inspector juga dapat diintegrasikan dengan Security Hub untuk

remediasi otomatis. Pertimbangkan untuk menerapkan jadwal tambalan reguler menggunakan Windows Pemeliharaan Manajer Sistem untuk meminimalkan gangguan pada instans Anda.

Instans Amazon EC2 memiliki kerentanan perangkat lunak

Paket perangkat lunak yang diinstal pada instans Amazon EC2 dapat terkena Common Vulnerabilities and Exposures (CVE). CVE nonkritis mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitabilitas yang lebih rendah dibandingkan dengan CVE kritis. Meskipun kerentanan ini menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Mengikuti praktik terbaik keamanan, tambal kerentanan ini untuk melindungi instans Anda dari serangan.

Remediasi: Perbarui instans yang terpengaruh

Gunakan AWS System Manager Patch Manager untuk menerapkan patch untuk sistem operasi. Patch Manager membantu Anda memilih dan menerapkan sistem operasi dan patch perangkat lunak secara otomatis pada kelompok instans yang besar. Jika Patch Manager tidak dikonfigurasi, perbarui sistem operasi secara manual pada setiap instans yang terpengaruh.

Perbarui aplikasi yang terpengaruh ke versi aman terbaru mengikuti prosedur yang direkomendasikan vendor. Untuk mengelola pembaruan aplikasi di beberapa instans, pertimbangkan untuk menggunakan AWS Manajer Status Manajer Sistem untuk menjaga perangkat lunak Anda dalam keadaan yang konsisten. Jika pembaruan tidak tersedia, pertimbangkan untuk menghapus atau menonaktifkan aplikasi rentan sampai patch dirilis atau mitigasi lainnya, seperti membatasi akses jaringan ke aplikasi atau menonaktifkan fitur rentan.

Ikuti saran remediasi khusus yang diberikan dalam temuan Inspektur Amazon. Ini bisa melibatkan perubahan aturan grup keamanan, memodifikasi konfigurasi instance, atau menyesuaikan pengaturan aplikasi.

Periksa apakah instance tersebut merupakan bagian dari Grup Penskalaan Otomatis. AMI-replacement tambalan dilakukan pada infrastruktur yang tidak dapat diubah dengan memperbarui ID AMI yang dikonfigurasi untuk menerapkan instans Amazon EC2 baru dalam grup Penskalaan Otomatis. Jika Anda menggunakan custom/golden AMI, buat instance dengan AMI baru, lalu sesuaikan instance dan buat AMI emas baru Untuk informasi selengkapnya, lihat tambalan pembaruan AMI (menggunakan AMI yang ditambal untuk grup Penskalaan Otomatis).

Pertimbangan masa depan

Untuk mencegah kejadian di masa mendatang, pertimbangkan untuk menerapkan program manajemen kerentanan. Amazon Inspector dapat dikonfigurasi untuk secara otomatis memindai CV pada instans Anda. Amazon Inspector juga dapat diintegrasikan dengan Security Hub untuk remediasi otomatis. Pertimbangkan untuk menerapkan jadwal tambalan reguler menggunakan Windows Pemeliharaan Manajer Sistem untuk meminimalkan gangguan pada instans Anda.

Instans EC2 memiliki sistem End-Of-Life operasi

Instans EC2 menjalankan sistem operasi akhir masa pakai yang tidak lagi didukung atau dikelola oleh pengembang asli. Ini mengekspos instance ke kerentanan keamanan dan potensi serangan. Ketika sistem operasi mencapai akhir masa pakai, vendor biasanya berhenti merilis saran keamanan baru. Nasihat keamanan yang ada juga dapat dihapus dari umpan vendor. Akibatnya, Amazon Inspector berpotensi berhenti menghasilkan temuan untuk CVE yang diketahui, menciptakan celah lebih lanjut dalam cakupan keamanan.

Lihat Sistem operasi yang dihentikan di Panduan Pengguna Amazon Inspector untuk informasi tentang sistem operasi yang telah mencapai akhir masa pakai yang dapat dideteksi oleh Amazon Inspector.

Remediasi: Perbarui ke versi sistem operasi yang didukung

Perbarui ke versi sistem operasi yang didukung. Dalam temuan eksposur, buka sumber daya untuk mengakses sumber daya yang terpengaruh. Sebelum memperbarui versi sistem operasi pada instans Anda, buat snapshot atau cadangan AMI jika Anda perlu memutar kembali. Kemudian, tinjau versi yang tersedia di Sistem Operasi yang Di dukung di Panduan Pengguna Amazon Inspector untuk daftar versi OS yang saat ini didukung.

Instans EC2 memiliki paket perangkat lunak berbahaya

Paket berbahaya adalah komponen perangkat lunak yang berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. Paket berbahaya menimbulkan ancaman aktif dan kritis terhadap instans Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan. Mengikuti praktik terbaik keamanan, hapus paket berbahaya untuk melindungi instans Anda dari potensi serangan.

Remediasi: Hapus paket berbahaya

Tinjau detail paket berbahaya di bagian Referensi tab Ker entanan sifat untuk memahami ancaman. Hapus paket berbahaya yang diidentifikasi menggunakan manajer paket yang sesuai.

Lihat Alat manajemen paket di Panduan Pengguna Amazon Linux 2023 untuk contoh. Setelah menghapus paket berbahaya, pertimbangkan untuk melakukan pemindaian untuk memastikan bahwa semua paket yang mungkin telah diinstal oleh kode berbahaya telah dihapus. Untuk informasi selengkapnya, lihat Memulai pemindaian On-demand malware GuardDuty di.

Instans EC2 memiliki file berbahaya

File berbahaya berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. File berbahaya menimbulkan ancaman aktif dan kritis terhadap instans Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan. Mengikuti praktik terbaik keamanan, hapus file berbahaya untuk melindungi instans Anda dari potensi serangan.

Remediasi: Hapus file berbahaya

Untuk mengidentifikasi volume Amazon Elastic Block Store (Amazon EBS) tertentu yang memiliki file berbahaya, tinjau bagian Sumber daya dari detail temuan sifat tersebut. Setelah Anda mengidentifikasi volume dengan file berbahaya, buat snapshot volume sebelum membuat perubahan, lalu hapus file berbahaya yang diidentifikasi. Setelah menghapus file berbahaya, pertimbangkan untuk melakukan pemindaian untuk memastikan bahwa semua file yang mungkin telah diinstal oleh file berbahaya telah dihapus. Untuk informasi selengkapnya, lihat Memulai pemindaian On-demand malware GuardDuty di.

Sifat dampak untuk instans EC2

Sifat dampak menggambarkan radius ledakan potensial dari suatu eksposur. Security Hub menganalisis izin efektif dari prinsipal yang terkait AWS Identity and Access Management dengan instans EC2 untuk menentukan sumber daya hilir yang dapat dijangkau penyerang jika instans dikompromikan. Setiap sifat dampak mengidentifikasi pola eskalasi hak istimewa tertentu. Untuk mengurangi radius ledakan Anda, tinjau jalur izin yang dijelaskan di setiap sifat dan hapus hak istimewa yang tidak perlu.

Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa paling sedikit dengan hanya memberikan izin yang diperlukan untuk melakukan tugas. Ganti kebijakan luas dengan kebijakan cakupan yang hanya memberikan tindakan dan sumber daya spesifik yang dibutuhkan. Untuk mengidentifikasi izin yang tidak digunakan untuk dihapus, gunakan Penganalisis Akses IAM untuk menghasilkan rekomendasi berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat Temuan untuk akses eksternal dan tidak digunakan dan M enerapkan izin hak istimewa terkecil di Panduan Pengguna IAM.

Memiliki jalur eksekutor istimewa kontrol penuh

Prinsipal terkait dapat meneruskan peran ke dan menyuntikkan kode ke sumber daya komputasi yang sudah memiliki izin tinggi. Hal ini memungkinkan prinsipal untuk mendapatkan kontrol penuh atas pelaksana dan melakukan tindakan apa pun yang diizinkan oleh peran pelaksana.

Memiliki jalur eskalasi kebijakan langsung

Prinsipal terkait dapat secara langsung memodifikasi kebijakan IAM untuk memberikan izin tambahan kepada dirinya sendiri, meningkatkan hak istimewanya sendiri tanpa sumber daya perantara.

Memiliki jalur pembajakan kebijakan kepercayaan

Prinsipal terkait dapat memodifikasi kebijakan kepercayaan dari peran IAM untuk membiarkan dirinya mengambil peran itu, mendapatkan izin peran tersebut.

Memiliki jalur data ransomware

Prinsipal terkait dapat mengenkripsi atau menghapus data dengan cara yang dapat digunakan untuk ransomware, seperti mengenkripsi objek Amazon S3 dengan kunci yang dikelola pelanggan dan kemudian memodifikasi kebijakan AWS KMS kunci.

Telah menghapus jalur pembatasan

Prinsipal terkait dapat menghapus batasan keamanan seperti batas izin, kebijakan kontrol layanan, atau pernyataan penolakan kebijakan berbasis sumber daya, memperluas apa yang dapat dilakukan oleh prinsipal lain atau sumber daya itu sendiri.

Memiliki jalur pass role buat eksekutor

Prinsipal terkait dapat membuat sumber daya komputasi baru (seperti fungsi Lambda atau instans Amazon EC2) dan memberikannya peran istimewa, secara efektif mencuci izinnya sendiri melalui sumber daya baru.

Memiliki jalur pelaksana peran swap yang ada

Prinsip terkait dapat mengubah peran IAM yang dilampirkan ke sumber daya komputasi yang ada, menggantinya dengan peran yang lebih istimewa untuk meningkatkan akses.

Memiliki jalur eskalasi rantai peran

Prinsipal terkait dapat mengambil urutan peran, di mana setiap peran dalam rantai memiliki izin yang semakin luas, pada akhirnya mencapai peran yang sangat istimewa.

Telah menyuntikkan jalur eksekutor istimewa kode

Prinsip terkait dapat menyuntikkan kode ke sumber daya komputasi yang sedang berjalan yang memiliki izin tinggi, menjalankan operasi arbitrer di bawah peran istimewa sumber daya tersebut.

Telah menonaktifkan jalur jejak audit

Prinsipal terkait dapat menonaktifkan layanan logging atau pemantauan seperti CloudTrail, secara efektif menutupi jejaknya selama atau setelah eskalasi.

Memiliki akses jalur eksekutor yang ada

Prinsipal terkait dapat memanggil atau menghubungkan ke sumber daya komputasi yang ada dan menggunakan peran terlampir untuk melakukan tindakan istimewa.

Memiliki jalur pencetakan kredensi

Prinsipal terkait dapat membuat kredenSIAL jangka panjang baru (seperti kunci akses atau profil login) untuk prinsipal lain, membuat jalur akses persisten yang bertahan dari rotasi kata sandi atau kedaluwarsa sesi.

Memiliki jalur akses data peran pass

Prinsipal terkait dapat membuat sumber daya layanan dan memberikannya peran yang memiliki akses ke data sensitif, mendapatkan akses tidak langsung ke data tersebut melalui sumber daya baru.

Memiliki jalur pembajakan tugas peran lulus

Prinsip terkait dapat meneruskan peran ke tugas yang dijadwalkan atau didorong oleh peristiwa (seperti fungsi Lambda yang dipicu oleh suatu peristiwa), memungkinkannya untuk mengeksekusi kode arbitrer dengan izin peran tersebut.

Memiliki jalur akses data hop tunggal

Prinsipal terkait dapat langsung mengakses sumber daya data sensitif (seperti bucket Amazon S3 atau tabel DynamoDB) melalui izin yang ada, tanpa memerlukan langkah eskalasi menengah.

Memiliki jalur kemajuan kemampuan

Prinsipal terkait memiliki jalur eskalasi hak istimewa yang memajukan kemampuan keseluruhannya melampaui apa yang disarankan oleh izin yang ditetapkan secara langsung. Ini adalah klasifikasi umum untuk jalur yang tidak cocok dengan pola yang lebih spesifik.

Memperbaiki eksposur untuk layanan Amazon ECS

AWS Security Hub dapat menghasilkan temuan eksposur untuk layanan Amazon Elastic Container Service (Amazon ECS).

Layanan Amazon ECS yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber daya dari detail temuan. Anda dapat mengambil detail sumber daya ini di konsol Hub Keamanan atau secara terprogram dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat kesalahan konfigurasi untuk layanan Amazon ECS
  - Layanan Amazon ECS menggunakan definisi tugas yang memungkinkan kontainer mengakses sistem file root
  - Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi untuk berbagi namespace proses host
  - Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan kredensional cleartext di variabel lingkungan
  - Layanan Amazon ECS memiliki grup keamanan terbuka
  - Layanan Amazon ECS memiliki alamat IP publik

- Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan mode jaringan host diaktifkan
- Sifat jangkauan untuk layanan Amazon ECS
  - Layanan Amazon ECS dapat dijangkau melalui internet
- Ciri-ciri kerentanan untuk layanan Amazon ECS
  - Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi
  - Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak
  - Layanan Amazon ECS memiliki wadah dengan sistem End-Of-Life operasi
  - Layanan Amazon ECS memiliki wadah dengan paket perangkat lunak berbahaya
- Sifat dampak untuk layanan Amazon ECS
  - Memiliki jalur eksekutor istimewa kontrol penuh
  - Memiliki jalur eskalasi kebijakan langsung
  - Memiliki jalur pembajakan kebijakan kepercayaan
  - Memiliki jalur data ransomware
  - Telah menghapus jalur pembatasan
  - Memiliki jalur pass role buat eksekutor
  - Memiliki jalur pelaksana peran swap yang ada
  - Memiliki jalur eskalasi rantai peran
  - Telah menyuntikkan jalur eksekutor istimewa kode
  - Telah menonaktifkan jalur jejak audit
  - Memiliki akses jalur eksekutor yang ada
  - Memiliki jalur pencetakan kredensi
  - Memiliki jalur akses data peran pass
  - Memiliki jalur pembajakan tugas peran lulus
  - Memiliki jalur akses data hop tunggal
  - Memiliki jalur kemajuan kemampuan

Sifat kesalahan konfigurasi untuk layanan Amazon ECS

Berikut adalah sifat kesalahan konfigurasi untuk layanan Amazon ECS dan langkah-langkah remediasi yang disarankan.

Layanan Amazon ECS menggunakan definisi tugas yang memungkinkan kontainer mengakses sistem file root

Kontainer Amazon ECS dengan akses ke sistem file root host berpotensi membaca, memodifikasi, atau mengeksekusi file penting pada sistem host. Konfigurasi ini meningkatkan risiko bahwa wadah yang dikompromikan dapat digunakan untuk mengakses atau memodifikasi sumber daya di luar cakupan yang dimaksudkan, berpotensi mengekspos data sensitif pada sistem file host. Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa terkecil, yang berarti Anda hanya memberikan izin yang diperlukan untuk melakukan tugas.

Remediasi: Tinjau dan modifikasi wadah dengan akses sistem file host

Dalam temuan eksposur, identifikasi definisi tugas ARN. Buka definisi tugas di konsol Amazon ECS. Cari bagian volume dalam definisi tugas yang mendefinisikan pemetaan jalur host.

Tinjau definisi tugas untuk menentukan apakah akses sistem file host diperlukan untuk fungsionalitas kontainer. Jika akses sistem file host tidak diperlukan, buat revisi definisi tugas baru dan hapus definisi volume yang menggunakan jalur host. Jika akses sistem file host diperlukan, pertimbangkan untuk mengonfigurasi wadah untuk menggunakan sistem file read-only untuk mencegah modifikasi yang tidak sah.

Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi untuk berbagi namespace proses host

Kontainer Amazon ECS yang berjalan dengan ruang nama yang terbuka berpotensi mengakses sumber daya sistem host dan ruang nama kontainer lainnya. Konfigurasi ini dapat memungkinkan wadah yang dikompromikan untuk keluar dari batas isolasi, mengakses proses, antarmuka jaringan, atau sumber daya lain di luar ruang lingkup yang dimaksudkan.

Namespace ID proses (PID) menyediakan pemisahan antar proses. Ini mencegah proses sistem terlihat, dan memungkinkan PID digunakan kembali, termasuk PID 1. Jika namespace PID host dibagikan dengan kontainer, kontainer dapat melihat semua proses pada sistem host, mengurangi isolasi tingkat proses. Hal ini dapat menyebabkan akses tidak sah ke proses host, termasuk kemampuan untuk memanipulasi dan menghentikannya. Mengikuti prinsip-prinsip keamanan standar, pertahankan isolasi namespace yang tepat untuk kontainer.

Remediasi: Perbarui definisi tugas dengan ruang nama yang terbuka

Buka tab Resources dari eksposur, identifikasi definisi tugas dengan namespace yang terbuka. Buka definisi tugas di konsol Amazon ECS. Cari pengaturan PIDMode dengan nilai host, yang akan

berbagi ruang nama ID proses dengan host. Hapus pengaturan PIDMode: host dari definisi tugas Anda untuk memastikan kontainer berjalan dengan isolasi namespace yang tepat.

Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan kredensional cleartext di variabel lingkungan

Kontainer Amazon ECS dengan kredensional cleartext dalam variabel lingkungan mengekspos informasi otentikasi sensitif yang dapat dikompromikan jika penyerang memperoleh akses ke definisi tugas, lingkungan kontainer, atau log kontainer. Ini menciptakan risiko keamanan yang signifikan, karena kredenSIAL yang bocor dapat digunakan untuk mengakses AWS layanan atau sumber daya lain.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Ganti kredensional cleartext

Dalam temuan eksposur, identifikasi definisi tugas dengan kredenSIAL cleartext. Buka definisi tugas di konsol Amazon ECS. Cari variabel lingkungan dalam definisi wadah yang berisi nilai-nilai sensitif seperti kunci AWS akses, kata sandi database, atau token API.

Pertimbangkan alternatif berikut untuk meneruskan kredenSIAL:

- Alih-alih menggunakan kunci AWS akses, gunakan peran eksekusi tugas IAM dan peran tugas untuk memberikan izin ke wadah Anda.
- Simpan kredenSIAL sebagai rahasia AWS Secrets Manager dan referensikan mereka dalam definisi tugas Anda.

Perbarui definisi tugas

Buat revisi baru dari definisi tugas Anda yang menangani kredenSIAL dengan aman. Kemudian perbarui layanan Amazon ECS Anda untuk menggunakan revisi definisi tugas baru.

Layanan Amazon ECS memiliki grup keamanan terbuka

Grup keamanan bertindak sebagai firewall virtual untuk tugas Amazon ECS Anda untuk mengontrol lalu lintas masuk dan keluar. Grup keamanan terbuka, yang memungkinkan akses tidak terbatas dari alamat IP apa pun, dapat mengekspos wadah Anda ke akses yang tidak sah, meningkatkan risiko paparan alat pemindaian otomatis dan serangan yang ditargetkan. Mengikuti prinsip keamanan standar, batasi akses grup keamanan ke alamat IP dan port tertentu.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau aturan grup keamanan dan menilai konfigurasi saat ini

Buka sumber daya untuk Grup Keamanan Amazon ECS. Evaluasi port mana yang terbuka dan dapat diakses dari rentang IP yang luas, seperti`(0.0.0.0/0 or ::/0)`.

Ubah aturan grup keamanan

Ubah aturan grup keamanan Anda untuk membatasi akses ke alamat atau rentang IP tepercaya tertentu. Saat memperbarui aturan grup keamanan Anda, pertimbangkan untuk memisahkan persyaratan akses untuk segmen jaringan yang berbeda dengan membuat aturan untuk setiap rentang IP sumber yang diperlukan atau membatasi akses ke port tertentu.

Ubah aturan grup keamanan

Pertimbangkan opsi berikut untuk metode akses alternatif:

- Session Manager menyediakan akses shell yang aman ke instans Amazon EC2 Anda tanpa perlu port masuk, mengelola kunci SSH, atau memelihara host bastion.
- NACL menyediakan lapisan keamanan tambahan di tingkat subnet. Tidak seperti grup keamanan, NACL bersifat stateless dan memerlukan aturan masuk dan keluar untuk didefinisikan secara eksplisit.

Layanan Amazon ECS memiliki alamat IP publik

Layanan Amazon ECS dengan alamat IP publik yang ditugaskan untuk tugas mereka dapat diakses langsung dari internet. Meskipun ini mungkin diperlukan untuk layanan yang perlu tersedia untuk umum, ini meningkatkan permukaan serangan dan potensi akses yang tidak sah.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Mengidentifikasi layanan dengan alamat IP publik

Dalam temuan eksposur, identifikasi layanan Amazon ECS yang memiliki alamat IP publik yang ditugaskan untuk tugasnya. Cari `assignPublicIp` pengaturan dengan nilai `ENABLED` dalam konfigurasi layanan.

Perbarui definisi tugas

Buat revisi baru dari definisi tugas Anda yang menonaktifkan alamat IP publik. Kemudian perbarui layanan Amazon ECS Anda untuk menggunakan revisi definisi tugas baru.

Menerapkan pola akses jaringan pribadi

Untuk contoh yang menjalankan aplikasi web, pertimbangkan untuk menggunakan Load Balancer (LB). LB dapat dikonfigurasi untuk memungkinkan instans Anda berjalan di subnet pribadi sementara LB berjalan di subnet publik dan menangani lalu lintas internet.

Layanan Amazon ECS menggunakan definisi tugas yang dikonfigurasi dengan mode jaringan host diaktifkan

Kontainer Amazon ECS yang berjalan dengan mode jaringan host berbagi namespace jaringan dengan host, memungkinkan akses langsung ke antarmuka jaringan host, port, dan tabel routing. Konfigurasi ini melewati isolasi jaringan yang disediakan oleh kontainer, berpotensi mengekspos layanan yang berjalan pada wadah langsung ke jaringan eksternal dan memungkinkan kontainer untuk mengubah pengaturan jaringan host. Mengikuti prinsip-prinsip keamanan standar, pertahankan isolasi jaringan yang tepat untuk kontainer.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Nonaktifkan mode jaringan host

Dalam temuan eksposur, identifikasi definisi tugas dengan mode jaringan host. Buka definisi tugas di konsol Amazon ECS. Cari pengaturan NetworkMode dengan nilai host dalam definisi tugas.

Pertimbangkan opsi berikut untuk menonaktifkan mode jaringan host:

- Mode `awsvpc` jaringan menyediakan tingkat isolasi jaringan terkuat dengan memberikan setiap tugas antarmuka jaringan elastisnya sendiri.
- Mode `bridge` jaringan menyediakan isolasi sambil memungkinkan pemetaan port untuk mengekspos port kontainer tertentu ke host.

Perbarui definisi tugas

Buat revisi baru dari definisi tugas Anda dengan konfigurasi mode jaringan yang diperbarui. Kemudian perbarui layanan Amazon ECS Anda untuk menggunakan revisi definisi tugas baru.

Sifat jangkauan untuk layanan Amazon ECS

Berikut adalah ciri-ciri jangkauan untuk layanan Amazon ECS dan langkah-langkah remediasi yang disarankan.

Layanan Amazon ECS dapat dijangkau melalui internet

Layanan Amazon ECS yang menjalankan tugas di subnet publik dapat diakses langsung dari internet. Ini meningkatkan permukaan serangan dan risiko akses yang tidak sah. Mengikuti prinsip-prinsip keamanan standar, jalankan tugas di subnet pribadi dan izinkan hanya akses internet yang diperlukan layanan Anda.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Menjalankan tugas di subnet pribadi

Untuk memindahkan tugas Anda dari subnet publik, perbarui konfigurasi jaringan untuk jenis peluncuran Anda:

- Untuk Fargate, tentukan subnet pribadi dalam konfigurasi jaringan layanan Amazon ECS Anda dan setel ke. `assignPublicIp` `DISABLED` Amazon ECS menghosting setiap tugas di subnet pribadi dan merutekan lalu lintas keluarnya melalui gateway NAT yang Anda kaitkan dengan subnet.
- Untuk EC2, luncurkan instance kontainer yang menyediakan kapasitas cluster Anda di subnet pribadi. Tugas menggunakan jaringan pribadi host dan merutekan lalu lintas keluar melalui gateway NAT.

Gunakan gateway NAT untuk akses keluar

Untuk tugas di subnet pribadi yang memerlukan akses internet keluar, gunakan gateway NAT. Anda dapat menggunakan gateway NAT untuk membiarkan tugas memulai koneksi keluar ke internet dan mencegah koneksi masuk dari internet. Untuk informasi selengkapnya, lihat Menghubungkan aplikasi Amazon ECS ke internet di Panduan Pengembang Amazon ECS.

Gunakan penyeimbang beban untuk akses masuk

Untuk layanan yang perlu menerima lalu lintas internet, jalankan tugas Anda di subnet pribadi di belakang penyeimbang beban yang berjalan di subnet publik. Untuk menambahkan perlindungan

terhadap eksploitasi web dan bot, kaitkan AWS Web Application Firewall (WAF) dengan penyeimbang beban Anda. Untuk informasi selengkapnya, lihat Menggunakan penyeimbangan beban untuk mendistribusikan lalu lintas layanan Amazon ECS di Panduan Pengembang Amazon ECS.

Ciri-ciri kerentanan untuk layanan Amazon ECS

Berikut adalah ciri-ciri kerentanan untuk Amazon ECS dan langkah-langkah perbaikan yang disarankan.

Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

1. Memahami eksposur

   Temuan kerentanan paket mengidentifikasi paket perangkat lunak di AWS lingkungan Anda yang terkena Kerentanan dan Eksposur Umum (CVE). Penyerang dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Gambar wadah ECR dapat memiliki temuan kerentanan paket.
2. Memperbaiki eksposur
   a. Perbarui versi paket

      Tinjau temuan kerentanan paket untuk gambar wadah ECR Anda. Perbarui versi paket seperti yang disarankan oleh Amazon Inspector. Untuk informasi selengkapnya, lihat Melihat detail untuk temuan Amazon Inspector Anda di Panduan Pengguna Amazon Inspector. Bagian Remediasi dari detail pencarian di konsol Amazon Inspector memberi tahu Anda perintah mana yang dapat Anda jalankan untuk memperbarui paket.

   b. Perbarui gambar wadah dasar

      Bangun kembali dan perbarui gambar wadah dasar secara teratur untuk menjaga kontainer Anda tetap mutakhir. Saat membangun kembali gambar, jangan sertakan komponen yang tidak perlu untuk mengurangi permukaan serangan. Untuk petunjuk tentang membangun kembali gambar kontainer, lihat Membangun kembali gambar Anda sesering mungkin.

Layanan Amazon ECS memiliki wadah dengan kerentanan perangkat lunak

Paket perangkat lunak yang diinstal pada wadah Amazon ECS dapat terkena Kerentanan dan Eksposur Umum (CVE). Kerentanan prioritas rendah mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitabilitas yang lebih rendah dibandingkan dengan kerentanan prioritas

tinggi. Meskipun kerentanan ini menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Perbarui gambar kontainer yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan pada sifat tersebut. Dokumentasi vendor mungkin mencakup panduan remediasi khusus.

Terapkan remediasi yang sesuai dengan mengikuti pedoman umum ini:

- Perbarui gambar kontainer Anda untuk menggunakan versi yang ditambal dari paket yang terpengaruh.
- Perbarui dependensi yang terpengaruh dalam aplikasi Anda ke versi aman terbaru.

Setelah memperbarui gambar kontainer Anda, dorong ke registri kontainer Anda dan perbarui definisi tugas Amazon ECS Anda untuk menggunakan gambar baru.

Pertimbangan masa depan

Untuk lebih memperkuat postur keamanan gambar kontainer Anda, pertimbangkan untuk mengikuti tugas Amazon ECS dan praktik terbaik keamanan kontainer. Amazon Inspector dapat dikonfigurasi untuk secara otomatis memindai CVE di wadah Anda. Amazon Inspector juga dapat diintegrasikan dengan Security Hub untuk remediasi otomatis. Pertimbangkan untuk menerapkan jadwal tambalan reguler menggunakan Windows Pemeliharaan Manajer Sistem untuk meminimalkan gangguan pada kontainer Anda.

Layanan Amazon ECS memiliki wadah dengan sistem End-Of-Life operasi

Kontainer Amazon ECS bergantung pada sistem operasi akhir masa pakai yang tidak lagi didukung atau dikelola oleh pengembang asli. Ini mengekspos wadah ke kerentanan keamanan dan potensi serangan. Ketika sistem operasi mencapai akhir masa pakai, vendor biasanya berhenti merilis saran keamanan baru. Nasihat keamanan yang ada juga dapat dihapus dari umpan vendor. Akibatnya, Amazon Inspector berpotensi berhenti menghasilkan temuan untuk CVE yang diketahui, menciptakan celah lebih lanjut dalam cakupan keamanan.

Lihat Sistem operasi yang dihentikan di Panduan Pengguna Amazon Inspector untuk informasi tentang sistem operasi yang telah mencapai akhir masa pakai yang dapat dideteksi oleh Amazon Inspector.

Remediasi: Perbarui ke versi sistem operasi yang didukung

Perbarui ke versi sistem operasi yang didukung. Dalam temuan eksposur, buka sumber daya untuk mengakses sumber daya yang terpengaruh. Sebelum memperbarui versi sistem operasi dalam image wadah Anda, tinjau versi yang tersedia di Sistem Operasi yang Didukung di Panduan Pengguna Amazon Inspector untuk daftar versi OS yang saat ini didukung. Setelah memperbarui gambar kontainer Anda, dorong ke registri kontainer Anda dan perbarui definisi tugas Amazon ECS Anda untuk menggunakan gambar baru.

Layanan Amazon ECS memiliki wadah dengan paket perangkat lunak berbahaya

Paket berbahaya adalah komponen perangkat lunak yang berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. Paket berbahaya menimbulkan ancaman aktif dan kritis terhadap gambar kontainer Amazon ECS Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan. Mengikuti praktik terbaik keamanan, hapus paket berbahaya untuk melindungi kontainer Anda dari potensi serangan.

Remediasi: Hapus paket berbahaya

Tinjau detail paket berbahaya di bagian Referensi tab Ker entanan sifat untuk memahami ancaman. Hapus paket berbahaya yang diidentifikasi dari gambar kontainer Anda lalu bangun kembali. Untuk informasi selengkapnya, lihat ContainerDependency Refer ensi API AWS Amazon ECS.

Setelah memperbarui gambar kontainer Anda, dorong ke registri kontainer Anda dan perbarui definisi tugas Amazon ECS Anda untuk menggunakan gambar baru. Untuk informasi selengkapnya, lihat Memperbarui definisi tugas Amazon ECS menggunakan konsol di Panduan Pengembang AWS Amazon ECS.

Sifat dampak untuk layanan Amazon ECS

Sifat dampak menggambarkan radius ledakan potensial dari suatu eksposur. Security Hub menganalisis izin efektif dari prinsipal yang AWS Identity and Access Management terkait dengan layanan Amazon ECS untuk menentukan sumber daya hilir yang dapat dijangkau penyerang jika

layanan dikompromikan. Setiap sifat dampak mengidentifikasi pola eskalasi hak istimewa tertentu. Untuk mengurangi radius ledakan Anda, tinjau jalur izin yang dijelaskan di setiap sifat dan hapus hak istimewa yang tidak perlu.

Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa paling sedikit dengan hanya memberikan izin yang diperlukan untuk melakukan tugas. Ganti kebijakan luas dengan kebijakan cakupan yang hanya memberikan tindakan dan sumber daya spesifik yang dibutuhkan. Untuk mengidentifikasi izin yang tidak digunakan untuk dihapus, gunakan Penganalisis Akses IAM untuk menghasilkan rekomendasi berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat Temuan untuk akses eksternal dan tidak digunakan dan M enerapkan izin hak istimewa terkecil di Panduan Pengguna IAM.

Memiliki jalur eksekutor istimewa kontrol penuh

Prinsipal terkait dapat meneruskan peran ke dan menyuntikkan kode ke sumber daya komputasi yang sudah memiliki izin tinggi. Hal ini memungkinkan prinsipal untuk mendapatkan kontrol penuh atas pelaksana dan melakukan tindakan apa pun yang diizinkan oleh peran pelaksana.

Memiliki jalur eskalasi kebijakan langsung

Prinsipal terkait dapat secara langsung memodifikasi kebijakan IAM untuk memberikan izin tambahan kepada dirinya sendiri, meningkatkan hak istimewanya sendiri tanpa sumber daya perantara.

Memiliki jalur pembajakan kebijakan kepercayaan

Prinsipal terkait dapat memodifikasi kebijakan kepercayaan dari peran IAM untuk membiarkan dirinya mengambil peran itu, mendapatkan izin peran tersebut.

Memiliki jalur data ransomware

Prinsipal terkait dapat mengenkripsi atau menghapus data dengan cara yang dapat digunakan untuk ransomware, seperti mengenkripsi objek Amazon S3 dengan kunci yang dikelola pelanggan dan kemudian memodifikasi kebijakan AWS KMS kunci.

Telah menghapus jalur pembatasan

Prinsipal terkait dapat menghapus batasan keamanan seperti batas izin, kebijakan kontrol layanan, atau pernyataan penolakan kebijakan berbasis sumber daya, memperluas apa yang dapat dilakukan oleh prinsipal lain atau sumber daya itu sendiri.

Memiliki jalur pass role buat eksekutor

Prinsipal terkait dapat membuat sumber daya komputasi baru (seperti fungsi Lambda atau instans Amazon EC2) dan memberikannya peran istimewa, secara efektif mencuci izinnya sendiri melalui sumber daya baru.

Memiliki jalur pelaksana peran swap yang ada

Prinsip terkait dapat mengubah peran IAM yang dilampirkan ke sumber daya komputasi yang ada, menggantinya dengan peran yang lebih istimewa untuk meningkatkan akses.

Memiliki jalur eskalasi rantai peran

Prinsipal terkait dapat mengambil urutan peran, di mana setiap peran dalam rantai memiliki izin yang semakin luas, pada akhirnya mencapai peran yang sangat istimewa.

Telah menyuntikkan jalur eksekutor istimewa kode

Prinsip terkait dapat menyuntikkan kode ke sumber daya komputasi yang sedang berjalan yang memiliki izin tinggi, menjalankan operasi arbitrer di bawah peran istimewa sumber daya tersebut.

Telah menonaktifkan jalur jejak audit

Prinsipal terkait dapat menonaktifkan layanan logging atau pemantauan seperti CloudTrail, secara efektif menutupi jejaknya selama atau setelah eskalasi.

Memiliki akses jalur eksekutor yang ada

Prinsipal terkait dapat memanggil atau menghubungkan ke sumber daya komputasi yang ada dan menggunakan peran terlampir untuk melakukan tindakan istimewa.

Memiliki jalur pencetakan kredensi

Prinsipal terkait dapat membuat kredenSIAL jangka panjang baru (seperti kunci akses atau profil login) untuk prinsipal lain, membuat jalur akses persisten yang bertahan dari rotasi kata sandi atau kedaluwarsa sesi.

Memiliki jalur akses data peran pass

Prinsipal terkait dapat membuat sumber daya layanan dan memberikannya peran yang memiliki akses ke data sensitif, mendapatkan akses tidak langsung ke data tersebut melalui sumber daya baru.

Memiliki jalur pembajakan tugas peran lulus

Prinsip terkait dapat meneruskan peran ke tugas yang dijadwalkan atau didorong oleh peristiwa (seperti fungsi Lambda yang dipicu oleh suatu peristiwa), memungkinkannya untuk mengeksekusi kode arbitrer dengan izin peran tersebut.

Memiliki jalur akses data hop tunggal

Prinsipal terkait dapat langsung mengakses sumber daya data sensitif (seperti bucket Amazon S3 atau tabel DynamoDB) melalui izin yang ada, tanpa memerlukan langkah eskalasi menengah.

Memiliki jalur kemajuan kemampuan

Prinsipal terkait memiliki jalur eskalasi hak istimewa yang memajukan kemampuan keseluruhannya melampaui apa yang disarankan oleh izin yang ditetapkan secara langsung. Ini adalah klasifikasi umum untuk jalur yang tidak cocok dengan pola yang lebih spesifik.

Memperbaiki eksposur untuk cluster Amazon EKS

AWS Security Hub dapat menghasilkan temuan eksposur untuk cluster Amazon Elastic Kubernetes Service (Amazon EKS).

Cluster Amazon EKS yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber Daya dari detail temuan. Anda dapat mengambil detail sumber daya ini di konsol Hub Keamanan atau secara terprogram dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat kesalahan konfigurasi untuk cluster Amazon EKS
  - Cluster Amazon EKS memungkinkan akses publik
  - Cluster Amazon EKS menggunakan versi Kubernetes yang tidak didukung
  - Cluster Amazon EKS menggunakan rahasia Kubernetes yang tidak terenkripsi
- Sifat kerentanan untuk cluster Amazon EKS
  - Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi
  - Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak
  - Cluster Amazon EKS memiliki wadah dengan sistem End-Of-Life operasi
  - Cluster Amazon EKS memiliki wadah dengan paket perangkat lunak berbahaya
  - Cluster Amazon EKS memiliki file berbahaya

Sifat kesalahan konfigurasi untuk cluster Amazon EKS

Berikut adalah sifat kesalahan konfigurasi untuk cluster Amazon EKS dan langkah-langkah remediasi yang disarankan.

Cluster Amazon EKS memungkinkan akses publik

Titik akhir cluster Amazon EKS adalah titik akhir yang Anda gunakan untuk berkomunikasi dengan server API Kubernetes cluster Anda. Secara default, titik akhir ini bersifat publik untuk internet. Titik akhir publik meningkatkan area permukaan serangan Anda dan risiko akses tidak sah ke server API Kubernetes Anda, yang berpotensi memungkinkan penyerang mengakses atau memodifikasi sumber daya cluster atau mengakses data sensitif. Mengikuti praktik terbaik keamanan, batasi akses ke titik akhir cluster Amazon EKS Anda hanya untuk rentang IP yang diperlukan.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Ubah akses titik akhir

Dalam temuan eksposur, buka sumber daya. Ini membuka cluster Amazon EKS yang terpengaruh. Anda dapat mengonfigurasi cluster Anda untuk menggunakan akses pribadi, akses publik, atau keduanya.

Dengan akses pribadi, permintaan API Kubernetes yang berasal dari VPC cluster Anda menggunakan titik akhir VPC pribadi. Dengan akses publik, permintaan API Kubernetes yang berasal dari luar VPC cluster Anda menggunakan titik akhir publik.

Memodifikasi atau hapus akses publik ke cluster

Untuk memodifikasi akses titik akhir untuk cluster yang ada, lihat Memo difikasi akses titik akhir cluster di Panduan Pengguna Layanan Amazon Elastic Kubernetes. Menerapkan aturan yang lebih ketat berdasarkan rentang IP atau grup keamanan tertentu. Jika akses publik terbatas diperlukan, batasi akses ke rentang blok CIDR tertentu atau gunakan daftar awalan.

Cluster Amazon EKS menggunakan versi Kubernetes yang tidak didukung

Amazon EKS mendukung setiap versi Kubernetes untuk jangka waktu terbatas. Menjalankan cluster dengan versi Kubernetes yang tidak didukung dapat mengekspos lingkungan Anda terhadap kerentanan keamanan, karena patch CVE akan berhenti dirilis untuk versi yang sudah ketinggalan zaman. Versi yang tidak didukung mungkin berisi kerentanan keamanan yang diketahui yang dapat dieksploitasi oleh penyerang dan tidak memiliki fitur keamanan yang mungkin tersedia di versi yang lebih baru. Mengikuti praktik terbaik keamanan, perbarui versi Kubernetes Anda.

Remediasi: Perbarui versi Kubernetes

Dalam temuan eksposur, buka sumber daya. Ini membuka cluster Amazon EKS yang terpengaruh. Sebelum memperbarui cluster Anda, tinjau versi yang tersedia pada dukungan standar di Panduan Pengguna Layanan Amazon Elastic Kubernetes untuk daftar versi Kubernetes yang saat ini didukung.

Cluster Amazon EKS menggunakan rahasia Kubernetes yang tidak terenkripsi

Rahasia Kubernetes, secara default, disimpan tanpa terenkripsi di penyimpanan data dasar server API (etcd). Siapa pun yang memiliki akses API atau dengan akses ke etcd dapat mengambil atau memodifikasi rahasia. Untuk mencegah hal ini, Anda harus mengenkripsi rahasia Kubernetes saat istirahat. Jika Rahasia Kubernetes tidak dienkripsi, mereka rentan terhadap akses tidak sah jika etcd dikompromikan. Karena rahasia sering mengandung informasi sensitif seperti kata sandi dan token

API, paparan mereka dapat menyebabkan akses tidak sah ke aplikasi dan data lain. Mengikuti praktik terbaik keamanan, mengenkripsi semua informasi sensitif yang disimpan dalam rahasia Kubernetes.

Remediasi: Enkripsi rahasia Kubernetes

Amazon EKS mendukung enkripsi rahasia Kubernetes menggunakan kunci KMS melalui enkripsi amplop. Untuk mengaktifkan enkripsi rahasia Kubernetes untuk cluster EKS Anda, lihat Mengen kripsi rahasia Kubernetes dengan KMS pada cluster yang ada di Panduan Pengguna Amazon EKS.

Sifat kerentanan untuk cluster Amazon EKS

Berikut adalah ciri-ciri kerentanan untuk cluster Amazon EKS.

Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

Paket perangkat lunak yang diinstal pada cluster Amazon EKS dapat terkena Common Vulnerabilities and Exposures (CVE). CVE kritis menimbulkan risiko keamanan yang signifikan bagi AWS lingkungan Anda. Pengguna yang tidak sah dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Kerentanan kritis dengan kemungkinan eksploitasi tinggi mewakili ancaman keamanan langsung, karena kode eksploitasi mungkin sudah tersedia untuk umum dan secara aktif digunakan oleh penyerang atau alat pemindaian otomatis. Mengikuti praktik terbaik keamanan, tambal kerentanan ini untuk melindungi instans Anda dari serangan.

Remediasi: Perbarui instans yang terpengaruh

Perbarui gambar kontainer Anda ke versi yang lebih baru yang menyertakan perbaikan keamanan untuk kerentanan yang teridentifikasi. Ini biasanya melibatkan membangun kembali gambar kontainer Anda dengan gambar dasar atau dependensi yang diperbarui, kemudian menerapkan gambar baru ke cluster Amazon EKS Anda.

Cluster Amazon EKS memiliki wadah dengan kerentanan perangkat lunak

Paket perangkat lunak yang diinstal pada cluster Amazon EKS dapat terkena Common Vulnerabilities and Exposures (CVE). CVE nonkritis mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitabilitas yang lebih rendah dibandingkan dengan CVE kritis. Meskipun kerentanan ini menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Mengikuti praktik terbaik keamanan, tambal kerentanan ini untuk melindungi instans Anda dari serangan.

Remediasi: Perbarui instans yang terpengaruh

Perbarui gambar kontainer Anda ke versi yang lebih baru yang menyertakan perbaikan keamanan untuk kerentanan yang teridentifikasi. Ini biasanya melibatkan membangun kembali gambar kontainer Anda dengan gambar dasar atau dependensi yang diperbarui, kemudian menerapkan gambar baru ke cluster Amazon EKS Anda.

Cluster Amazon EKS memiliki wadah dengan sistem End-Of-Life operasi

Gambar wadah Amazon EKS bergantung pada sistem operasi akhir masa pakai yang tidak lagi didukung atau dikelola oleh pengembang asli. Ini mengekspos wadah ke kerentanan keamanan dan potensi serangan. Ketika sistem operasi mencapai akhir masa pakai, vendor biasanya berhenti merilis saran keamanan baru. Nasihat keamanan yang ada juga dapat dihapus dari umpan vendor. Akibatnya, Amazon Inspector berpotensi berhenti menghasilkan temuan untuk CVE yang diketahui, menciptakan celah lebih lanjut dalam cakupan keamanan.

Lihat Sistem operasi yang dihentikan di Panduan Pengguna Amazon Inspector untuk informasi tentang sistem operasi yang telah mencapai akhir masa pakai yang dapat dideteksi oleh Amazon Inspector.

Remediasi: Perbarui ke versi sistem operasi yang didukung

Perbarui ke versi sistem operasi yang didukung. Dalam temuan eksposur, buka sumber daya untuk mengakses sumber daya yang terpengaruh. Sebelum memperbarui versi sistem operasi dalam image wadah Anda, tinjau versi yang tersedia di Sistem Operasi yang Didukung di Panduan Pengguna Amazon Inspector untuk daftar versi OS yang saat ini didukung. Setelah memperbarui gambar kontainer Anda, bangun kembali dan gunakan kembali kontainer Anda ke cluster Amazon EKS.

Cluster Amazon EKS memiliki wadah dengan paket perangkat lunak berbahaya

Paket berbahaya adalah komponen perangkat lunak yang berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. Paket berbahaya menimbulkan ancaman aktif dan kritis bagi cluster Amazon EKS Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan. Mengikuti praktik terbaik keamanan, hapus paket berbahaya untuk melindungi cluster Anda dari potensi serangan.

Remediasi: Hapus paket berbahaya

Tinjau detail paket berbahaya di bagian Referensi tab Ker entanan sifat untuk memahami ancaman. Hapus paket berbahaya yang diidentifikasi dari gambar kontainer Anda. Kemudian, hapus pod dengan gambar yang dikompromikan.

Perbarui penerapan Kubernetes Anda untuk menggunakan gambar kontainer yang diperbarui. Kemudian, terapkan perubahan Anda dan gunakan kembali pod Anda.

Cluster Amazon EKS memiliki file berbahaya

File berbahaya berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. File berbahaya menimbulkan ancaman aktif dan kritis bagi cluster Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan. Mengikuti praktik terbaik keamanan, hapus file berbahaya untuk melindungi cluster Anda dari potensi serangan.

Remediasi: Hapus file berbahaya

Untuk mengidentifikasi volume Amazon Elastic Block Store (Amazon EBS) tertentu yang memiliki file berbahaya, tinjau bagian Sumber daya dari detail temuan sifat tersebut. Setelah Anda mengidentifikasi volume dengan file berbahaya, hapus file berbahaya yang diidentifikasi. Setelah menghapus file berbahaya, pertimbangkan untuk melakukan pemindaian untuk memastikan bahwa semua file yang mungkin telah diinstal oleh file berbahaya telah dihapus. Untuk informasi selengkapnya, lihat Memulai pemindaian On-demand malware GuardDuty di.

Memperbaiki eksposur untuk pengguna IAM

AWS Security Hub dapat menghasilkan temuan eksposur untuk pengguna AWS Identity and Access Management (IAM).

Pada konsol Hub Keamanan, pengguna IAM yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber Daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan

menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Praktik terbaik IAM menyarankan Anda membuat peran IAM atau menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredentif sementara alih-alih membuat pengguna IAM individual. Jika itu adalah opsi untuk organisasi dan kasus penggunaan Anda, beralihlah ke peran atau federasi alih-alih menggunakan pengguna IAM. Untuk informasi selengkapnya, lihat Pengguna IAM di Panduan Pengguna IAM.

Daftar Isi

- Sifat kesalahan konfigurasi untuk pengguna IAM
  - Pengguna IAM tidak mengaktifkan MFA
  - Bagian AWS akun untuk pengguna IAM memiliki kebijakan kata sandi yang lemah
  - Pengguna IAM memiliki kunci akses yang tidak diputar
  - Pengguna IAM memiliki kebijakan yang memungkinkan akses tak terbatas ke dekripsi kunci KMS
- Sifat akses yang tidak digunakan untuk pengguna IAM
- Sifat dampak untuk pengguna IAM
  - Memiliki jalur eksekutor istimewa kontrol penuh
  - Memiliki jalur eskalasi kebijakan langsung
  - Memiliki jalur pembajakan kebijakan kepercayaan
  - Memiliki jalur data ransomware
  - Telah menghapus jalur pembatasan
  - Memiliki jalur pass role buat eksekutor
  - Memiliki jalur pelaksana peran swap yang ada
  - Memiliki jalur eskalasi rantai peran
  - Telah menyuntikkan jalur eksekutor istimewa kode
  - Telah menonaktifkan jalur jejak audit
  - Memiliki akses jalur eksekutor yang ada

- Memiliki jalur pencetakan kredensi
- Memiliki jalur akses data peran pass
- Memiliki jalur pembajakan tugas peran lulus
- Memiliki jalur akses data hop tunggal
- Memiliki jalur kemajuan kemampuan

Sifat kesalahan konfigurasi untuk pengguna IAM

Berikut adalah sifat kesalahan konfigurasi untuk pengguna IAM dan langkah-langkah remediasi yang disarankan.

Pengguna IAM tidak mengaktifkan MFA

Multi-factor otentikasi (MFA) menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Ketika MFA diaktifkan dan pengguna IAM masuk ke AWS situs web, mereka diminta untuk memasukkan nama pengguna, kata sandi, dan kode otentikasi dari perangkat AWS MFA mereka. Prinsipal otentikasi harus memiliki perangkat yang memancarkan kunci sensitif waktu dan harus memiliki pengetahuan tentang kredensi. Tanpa MFA, jika kata sandi pengguna dikompromikan, penyerang mendapatkan akses penuh ke AWS izin pengguna. Mengikuti prinsip keamanan standar, aktifkan MFA untuk semua akun dan pengguna yang memiliki Konsol Manajemen AWS akses.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau jenis MFA

AWS mendukung jenis https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html#id_credentials_mfa-types MFA berikut:

- Kunci sandi dan kunci keamanan
- Aplikasi otentikator virtual
- Token TOTP perangkat keras

Meskipun otentikasi dengan perangkat fisik biasanya memberikan perlindungan keamanan yang lebih ketat, menggunakan semua jenis MFA lebih aman daripada menonaktifkan MFA.

Aktifkan MFA

Untuk mengaktifkan jenis MFA yang sesuai dengan kebutuhan Anda, lihat otentikasi AWS multi-faktor di IAM di Panduan Pengguna IAM. Ikuti langkah-langkah untuk jenis MFA tertentu yang ingin Anda terapkan. Untuk organisasi yang mengelola banyak pengguna, Anda mungkin ingin menerapkan penggunaan MFA dengan mewajibkan MFA untuk mengakses sumber daya sensitif.

Bagian AWS akun untuk pengguna IAM memiliki kebijakan kata sandi yang lemah

Kebijakan kata sandi membantu melindungi dari akses yang tidak sah dengan menegakkan persyaratan kompleksitas minimum untuk kata sandi pengguna IAM. Tanpa kebijakan kata sandi yang kuat, ada peningkatan risiko bahwa akun pengguna dapat dikompromikan melalui tebakan kata sandi atau serangan brute force. Mengikuti prinsip-prinsip keamanan standar, terapkan kebijakan kata sandi yang kuat untuk memastikan pengguna membuat kata sandi kompleks yang sulit ditebak.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Konfigurasikan kebijakan kata sandi yang kuat

Buka dasbor IAM dan navigasikan ke Pengaturan akun. Tinjau setelan kebijakan kata sandi saat ini untuk akun Anda, termasuk panjang minimum, jenis karakter yang diperlukan, dan setelan kedaluwarsa kata sandi.

Minimal, ikuti praktik terbaik berikut saat menetapkan kebijakan kata sandi Anda:

- Memerlukan setidaknya satu karakter huruf besar.
- Memerlukan setidaknya satu karakter huruf kecil.
- Memerlukan setidaknya satu simbol.
- Memerlukan setidaknya satu nomor.
- Memerlukan setidaknya delapan karakter.

Pertimbangan keamanan tambahan

Pertimbangkan langkah-langkah keamanan tambahan ini selain kebijakan kata sandi yang kuat:

- MFA menambahkan lapisan keamanan tambahan dengan memerlukan bentuk otentikasi tambahan. Ini membantu mencegah akses yang tidak sah bahkan jika kredenSIAL dikompromikan.
- Menyiapkan elemen kondisi untuk membatasi kapan dan bagaimana izin administratif dapat digunakan berdasarkan faktor-faktor seperti IP sumber atau usia MFA.

Pengguna IAM memiliki kunci akses yang tidak diputar

Kunci akses terdiri dari ID kunci akses dan kunci akses rahasia yang memungkinkan akses terprogram ke AWS sumber daya. Ketika kunci akses tetap tidak berubah untuk jangka waktu yang lama, mereka meningkatkan risiko akses tidak sah jika dikompromikan. Mengikuti praktik terbaik keamanan, putar kunci akses setiap 90 hari untuk meminimalkan jendela peluang bagi penyerang untuk menggunakan kredenSIAL yang dikompromikan.

Remediasi: Putar tombol akses

Dalam temuan eksposur, buka sumber daya. Ini membuka jendela detail pengguna. Untuk memutar kunci akses, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Pengguna IAM memiliki kebijakan yang memungkinkan akses tak terbatas ke dekripsi kunci KMS

AWS KMS memungkinkan Anda untuk membuat dan mengelola kunci kriptografi yang digunakan untuk melindungi data Anda. Kebijakan IAM yang mengizinkan izin AWS KMS dekripsi tak terbatas (misalnya, `kms:Decrypt` atau`kms:ReEncryptFrom`) pada semua kunci KMS dapat menyebabkan akses data yang tidak sah jika kredentif pengguna IAM dikompromikan. Jika penyerang mendapatkan akses ke kredenSIAL ini, mereka berpotensi mendekripsi data terenkripsi apa pun di lingkungan Anda, yang dapat mencakup data sensitif. Mengikuti praktik terbaik keamanan, terapkan hak istimewa terkecil dengan membatasi izin AWS KMS dekripsi hanya untuk kunci tertentu yang dibutuhkan pengguna untuk fungsi pekerjaan mereka.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Menerapkan akses hak istimewa yang paling rendah

Dalam temuan eksposur, buka sumber daya. Ini membuka jendela Kebijakan IAM. Cari izin di KMS yang memungkinkan KMS:Decrypt atau `kms:ReEncryptFrom` atau `KMS:*` dengan spesifikasi sumber daya. `"*"`

Perbarui kebijakan untuk membatasi izin AWS KMS dekripsi hanya pada kunci tertentu yang diperlukan. Ubah kebijakan untuk mengganti `"*"` sumber daya dengan ARN spesifik AWS KMS kunci yang diperlukan.

Pertimbangan konfigurasi aman

Pertimbangkan untuk menambahkan kondisi untuk membatasi lebih lanjut kapan izin ini dapat digunakan. Misalnya, Anda dapat membatasi operasi dekripsi ke titik akhir VPC tertentu atau rentang

IP sumber. Anda juga dapat mengonfigurasi kebijakan kunci untuk lebih membatasi siapa yang dapat menggunakan kunci KMS tertentu.

Sifat akses yang tidak digunakan untuk pengguna IAM

Ketika pengguna IAM memiliki izin, kunci akses, atau kata sandi yang tidak digunakan, Security Hub dapat menyertakan ini sebagai sifat kontekstual dalam temuan eksposur untuk pengguna tersebut. Ciri-ciri ini dihasilkan oleh Penganalisis Akses IAM yang dikelola layanan dan memberikan konteks tambahan tentang postur keamanan pengguna. Sifat akses yang tidak digunakan bukanlah penyebab utama temuan eksposur, tetapi mereka menunjukkan bahwa pengguna memiliki lebih banyak izin daripada yang diperlukan, yang meningkatkan dampak potensial jika kredenSIAL pengguna dikompromikan.

Khususnya untuk izin yang tidak digunakan, Anda dapat membuat rekomendasi kebijakan hak istimewa terendah yang menunjukkan kebijakan penggantian dengan cakupan. Untuk informasi selengkapnya, lihat the section called “Rekomendasi kebijakan”.

Sifat dampak untuk pengguna IAM

Sifat dampak menggambarkan radius ledakan potensial dari suatu eksposur. Security Hub menganalisis izin efektif dari prinsipal yang terkait AWS Identity and Access Management dengan pengguna IAM untuk menentukan sumber daya hilir yang dapat dijangkau penyerang jika pengguna IAM dikompromikan. Setiap sifat dampak mengidentifikasi pola eskalasi hak istimewa tertentu. Untuk mengurangi radius ledakan Anda, tinjau jalur izin yang dijelaskan di setiap sifat dan hapus hak istimewa yang tidak perlu.

Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa paling sedikit dengan hanya memberikan izin yang diperlukan untuk melakukan tugas. Ganti kebijakan luas dengan kebijakan cakupan yang hanya memberikan tindakan dan sumber daya spesifik yang dibutuhkan. Untuk mengidentifikasi izin yang tidak digunakan untuk dihapus, gunakan Penganalisis Akses IAM untuk menghasilkan rekomendasi berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat Temuan untuk akses eksternal dan tidak digunakan dan M enerapkan izin hak istimewa terkecil di Panduan Pengguna IAM.

Memiliki jalur eksekutor istimewa kontrol penuh

Prinsipal terkait dapat meneruskan peran ke dan menyuntikkan kode ke sumber daya komputasi yang sudah memiliki izin tinggi. Hal ini memungkinkan prinsipal untuk mendapatkan kontrol penuh atas pelaksana dan melakukan tindakan apa pun yang diizinkan oleh peran pelaksana.

Memiliki jalur eskalasi kebijakan langsung

Prinsipal terkait dapat secara langsung memodifikasi kebijakan IAM untuk memberikan izin tambahan kepada dirinya sendiri, meningkatkan hak istimewanya sendiri tanpa sumber daya perantara.

Memiliki jalur pembajakan kebijakan kepercayaan

Prinsipal terkait dapat memodifikasi kebijakan kepercayaan dari peran IAM untuk membiarkan dirinya mengambil peran itu, mendapatkan izin peran tersebut.

Memiliki jalur data ransomware

Prinsipal terkait dapat mengenkripsi atau menghapus data dengan cara yang dapat digunakan untuk ransomware, seperti mengenkripsi objek Amazon S3 dengan kunci yang dikelola pelanggan dan kemudian memodifikasi kebijakan AWS KMS kunci.

Telah menghapus jalur pembatasan

Prinsipal terkait dapat menghapus batasan keamanan seperti batas izin, kebijakan kontrol layanan, atau pernyataan penolakan kebijakan berbasis sumber daya, memperluas apa yang dapat dilakukan oleh prinsipal lain atau sumber daya itu sendiri.

Memiliki jalur pass role buat eksekutor

Prinsipal terkait dapat membuat sumber daya komputasi baru (seperti fungsi Lambda atau instans Amazon EC2) dan memberikannya peran istimewa, secara efektif mencuci izinnya sendiri melalui sumber daya baru.

Memiliki jalur pelaksana peran swap yang ada

Prinsip terkait dapat mengubah peran IAM yang dilampirkan ke sumber daya komputasi yang ada, menggantinya dengan peran yang lebih istimewa untuk meningkatkan akses.

Memiliki jalur eskalasi rantai peran

Prinsipal terkait dapat mengambil urutan peran, di mana setiap peran dalam rantai memiliki izin yang semakin luas, pada akhirnya mencapai peran yang sangat istimewa.

Telah menyuntikkan jalur eksekutor istimewa kode

Prinsip terkait dapat menyuntikkan kode ke sumber daya komputasi yang sedang berjalan yang memiliki izin tinggi, menjalankan operasi arbitrer di bawah peran istimewa sumber daya tersebut.

Telah menonaktifkan jalur jejak audit

Prinsipal terkait dapat menonaktifkan layanan logging atau pemantauan seperti CloudTrail, secara efektif menutupi jejaknya selama atau setelah eskalasi.

Memiliki akses jalur eksekutor yang ada

Prinsipal terkait dapat memanggil atau menghubungkan ke sumber daya komputasi yang ada dan menggunakan peran terlampir untuk melakukan tindakan istimewa.

Memiliki jalur pencetakan kredensi

Prinsipal terkait dapat membuat kredenSIAL jangka panjang baru (seperti kunci akses atau profil login) untuk prinsipal lain, membuat jalur akses persisten yang bertahan dari rotasi kata sandi atau kedaluwarsa sesi.

Memiliki jalur akses data peran pass

Prinsipal terkait dapat membuat sumber daya layanan dan memberikannya peran yang memiliki akses ke data sensitif, mendapatkan akses tidak langsung ke data tersebut melalui sumber daya baru.

Memiliki jalur pembajakan tugas peran lulus

Prinsip terkait dapat meneruskan peran ke tugas yang dijadwalkan atau didorong oleh peristiwa (seperti fungsi Lambda yang dipicu oleh suatu peristiwa), memungkinkannya untuk mengeksekusi kode arbitrer dengan izin peran tersebut.

Memiliki jalur akses data hop tunggal

Prinsipal terkait dapat langsung mengakses sumber daya data sensitif (seperti bucket Amazon S3 atau tabel DynamoDB) melalui izin yang ada, tanpa memerlukan langkah eskalasi menengah.

Memiliki jalur kemajuan kemampuan

Prinsipal terkait memiliki jalur eskalasi hak istimewa yang memajukan kemampuan keseluruhannya melampaui apa yang disarankan oleh izin yang ditetapkan secara langsung. Ini adalah klasifikasi umum untuk jalur yang tidak cocok dengan pola yang lebih spesifik.

Memperbaiki eksposur untuk AWS Lambda fungsi

AWS Security Hub dapat menghasilkan temuan eksposur untuk AWS Lambda fungsi.

Pada konsol Hub Keamanan, fungsi Lambda yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber Daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat salah konfigurasi untuk fungsi Lambda
  - Fungsi Lambda digunakan di luar Amazon VPC
  - Fungsi Lambda dapat diakses melalui API Gateway tanpa otorisasi
- Sifat jangkauan untuk fungsi Lambda
  - Fungsi Lambda dapat dipanggil secara publik
- Sifat kerentanan untuk fungsi Lambda
  - Fungsi Lambda memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan
  - Fungsi Lambda memiliki kerentanan perangkat lunak
  - Fungsi Lambda memiliki paket perangkat lunak berbahaya
  - Fungsi Lambda memiliki kerentanan kode
- Sifat dampak untuk fungsi Lambda
  - Memiliki jalur eksekutor istimewa kontrol penuh
  - Memiliki jalur eskalasi kebijakan langsung

- Memiliki jalur pembajakan kebijakan kepercayaan
- Memiliki jalur data ransomware
- Telah menghapus jalur pembatasan
- Memiliki jalur pass role buat eksekutor
- Memiliki jalur pelaksana peran swap yang ada
- Memiliki jalur eskalasi rantai peran
- Telah menyuntikkan jalur eksekutor istimewa kode
- Telah menonaktifkan jalur jejak audit
- Memiliki akses jalur eksekutor yang ada
- Memiliki jalur pencetakan kredensi
- Memiliki jalur akses data peran pass
- Memiliki jalur pembajakan tugas peran lulus
- Memiliki jalur akses data hop tunggal
- Memiliki jalur kemajuan kemampuan

Sifat salah konfigurasi untuk fungsi Lambda

Berikut adalah sifat kesalahan konfigurasi untuk fungsi Lambda dan langkah-langkah remediasi yang disarankan.

Fungsi Lambda digunakan di luar Amazon VPC

Fungsi lambda secara default digunakan dengan akses ke internet publik. Konfigurasi default ini memberi fungsi Lambda kemampuan untuk mencapai titik AWS akhir layanan dan API eksternal, tetapi juga mengekspos mereka pada potensi risiko keamanan. Fungsi dengan akses internet dapat digunakan untuk mengeksfiltrasi data, berkomunikasi dengan server yang tidak sah, atau menjadi titik masuk bagi aktor eksternal jika dikompromikan. Amazon VPC menyediakan isolasi jaringan dengan membatasi fungsi Lambda Anda untuk berkomunikasi hanya dengan sumber daya dalam jaringan pribadi yang Anda tentukan. Mengikuti prinsip-prinsip keamanan standar, gunakan fungsi Lambda dalam VPC untuk meningkatkan keamanan melalui isolasi jaringan.

Remediasi: Lampirkan fungsi ke VPC

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka fungsi Lambda di konsol Lambda. Untuk mengamankan fungsi Lambda Anda dengan membatasi akses jaringannya, lampirkan ke VPC yang memiliki kontrol jaringan yang sesuai.

Sebelum melampirkan fungsi Anda ke VPC, rencanakan akses AWS layanan apa pun yang mungkin diperlukan, karena fungsi di subnet pribadi tanpa gateway NAT atau titik akhir VPC tidak dapat mencapai API layanan. AWS Untuk informasi tentang cara melampirkan fungsi Lambda ke Amazon VPC di akun Anda, lihat Melampirkan fungsi Lambda ke Amazon VPC di akun Anda. Akun AWS Pertimbangkan untuk menggunakan titik akhir VPC untuk konektivitas layanan tanpa akses internet jika fungsi Anda mengharuskan untuk mengakses AWS layanan dari dalam subnet pribadi. Konfigurasikan NAT Gateway jika Anda memerlukan konektivitas internet keluar dari subnet pribadi.

Fungsi Lambda dapat diakses melalui API Gateway tanpa otorisasi

Metode API Gateway tanpa otorisasi memungkinkan pemanggil dengan akses ke API Gateway untuk memanggil fungsi Lambda terintegrasi tanpa verifikasi identitas. Konfigurasi ini menciptakan risiko keamanan, karena pemanggil dapat memanggil fungsi Lambda tanpa otorisasi yang tepat, yang berpotensi menyebabkan penyalahgunaan kemampuan fungsi, konsumsi sumber daya, akses ke data sensitif, atau operasi yang tidak sah. Sementara API Gateway mungkin memiliki kontrol akses tingkat jaringan, kurangnya otorisasi tingkat metode dapat memungkinkan pemanggilan fungsi secara gratis oleh pemanggil mana pun dengan akses jaringan ke API Gateway. Mengikuti praktik terbaik keamanan, terapkan mekanisme otorisasi yang sesuai untuk metode API Gateway yang terintegrasi dengan fungsi Lambda.

Remediasi: Konfigurasikan otentikasi API Gateway

Di tab Resources pada eksposur, pilih tautan sumber daya untuk mengakses metode API Gateway. Tinjau konfigurasi otorisasi saat ini dan terapkan mekanisme otentikasi yang sesuai.

API Gateway mendukung beberapa opsi otentikasi termasuk AWS IAM, Amazon Cognito User Pools, Lambda Authorizers, dan API keys. Pilih metode otentikasi yang paling sesuai dengan persyaratan keamanan dan kasus penggunaan Anda. Untuk petunjuk terperinci tentang mengonfigurasi otentikasi, lihat Mengon trol dan mengelola akses ke REST API di API Gateway di Panduan Pengembang API Gateway.

Sifat jangkauan untuk fungsi Lambda

Berikut adalah ciri-ciri jangkauan untuk fungsi Lambda dan langkah-langkah remediasi yang disarankan.

Fungsi Lambda dapat dipanggil secara publik

Kebijakan berbasis sumber daya Lambda menentukan siapa yang dapat memanggil fungsi Anda. Fungsi dengan kebijakan sumber daya yang menyertakan “*” sebagai prinsipal (atau tidak ada

prinsipal sama sekali) memungkinkan AWS pengguna yang diautentikasi untuk memanggilnya. Hal ini menciptakan risiko yang signifikan, terutama untuk fungsi yang memproses data sensitif, memodifikasi sumber daya, atau memiliki izin yang lebih tinggi. Pengguna yang tidak sah dapat mengeksploitasi konfigurasi ini untuk melakukan operasi yang tidak diinginkan, berpotensi mengekspos data, memanipulasi sumber daya, atau menyalahgunakan kemampuan fungsi. Mengikuti praktik terbaik keamanan, batasi akses fungsi Lambda hanya untuk prinsipal resmi.

Remediasi: Ubah kebijakan berbasis sumber daya fungsi

Di tab Sumber daya eksposur, buka sumber daya dengan hyperlink. Ini membuka fungsi Lambda di konsol Lambda. Batasi akses ke fungsi Lambda Anda dengan menetapkan hanya ID AWS akun resmi atau prinsipal IAM tertentu (pengguna, peran, atau layanan) dalam kebijakan berbasis sumber daya. Anda hanya dapat mengubah kebijakan berbasis sumber daya secara terprogram.

Sifat kerentanan untuk fungsi Lambda

Berikut adalah ciri-ciri kerentanan untuk fungsi Lambda dan langkah-langkah remediasi yang disarankan.

Fungsi Lambda memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan

Paket perangkat lunak yang digunakan dalam kode fungsi Lambda dapat berisi Kerentanan Umum dan Eksposur (CVE) yang memiliki peluang tinggi untuk dieksploitasi. CVE kritis menimbulkan risiko keamanan yang signifikan bagi AWS lingkungan Anda. Penyerang dapat mengeksploitasi kerentanan yang belum ditambal ini untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Kerentanan kritis dengan kemungkinan eksploitasi tinggi mewakili ancaman keamanan langsung, karena kode eksploitasi mungkin sudah tersedia untuk umum dan secara aktif digunakan oleh penyerang atau alat pemindaian otomatis. Mengikuti praktik terbaik keamanan, tambal kerentanan ini untuk melindungi fungsi Anda dari serangan.

Remediasi: Perbarui fungsi yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan untuk sifat tersebut. Dokumentasi vendor mungkin mencakup panduan remediasi khusus. Perbarui pustaka rentan ke versi aman terbaru mereka mengikuti prosedur yang direkomendasikan vendor.

Biasanya, alur kerja remediasi tergantung pada apakah Anda menerapkan paket Lambda dengan mengunggah file zip atau dengan membuat fungsi Lambda dengan image wadah. Setelah memperbarui pustaka, perbarui kode fungsi Lambda untuk menggunakan versi tetap. Setelah itu, gunakan versi yang diperbarui.

Fungsi Lambda memiliki kerentanan perangkat lunak

Fungsi lambda sering menggunakan pustaka dan dependensi pihak ketiga yang mungkin berisi kerentanan keamanan dengan tingkat keparahan atau eksploitabilitas yang lebih rendah dibandingkan dengan CVE kritis. Meskipun kerentanan non-kritis ini mungkin tidak dapat dieksploitasi segera, mereka masih mewakili kelemahan keamanan yang dapat dirantai bersama dengan kerentanan lain untuk membahayakan fungsi Anda. Seiring waktu, teknik eksploitasi baru mungkin juga muncul yang meningkatkan risiko kerentanan ini. Mengikuti prinsip-prinsip keamanan standar, tambal kerentanan ini untuk menjaga lingkungan yang aman.

Remediasi: Perbarui fungsi yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan untuk sifat tersebut. Dokumentasi vendor mungkin mencakup panduan remediasi khusus. Perbarui pustaka rentan ke versi aman terbaru mereka mengikuti prosedur yang direkomendasikan vendor.

Biasanya, alur kerja remediasi tergantung pada apakah Anda menerapkan paket Lambda dengan mengunggah file zip atau dengan membuat fungsi Lambda dengan image wadah. Setelah memperbarui pustaka, perbarui kode fungsi Lambda untuk menggunakan versi tetap. Setelah itu, gunakan versi yang diperbarui.

Fungsi Lambda memiliki paket perangkat lunak berbahaya

Paket berbahaya adalah komponen perangkat lunak yang berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. Paket berbahaya menimbulkan ancaman aktif dan kritis terhadap fungsi Lambda Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan. Mengikuti praktik terbaik keamanan, hapus paket berbahaya untuk melindungi fungsi Lambda Anda dari potensi serangan.

Remediasi: Hapus paket berbahaya

Tinjau detail paket berbahaya di bagian Referensi tab Ker entanan sifat untuk memahami ancaman. Hapus paket berbahaya yang diidentifikasi dari kode fungsi dan dependensi Anda. Untuk fungsi yang menggunakan lapisan, periksa apakah paket berbahaya diinstal di lapisan apa pun dan hapus.

Perbarui paket penerapan atau image kontainer Anda untuk mengecualikan paket berbahaya, lalu terapkan versi yang diperbarui. Untuk petunjuk, lihat Menye barkan fungsi Lambda sebagai arsip

berkas.zip untuk arsip file.zip atau Membuat fungsi Lambda menggunakan gambar kontainer untuk gambar kontainer.

Fungsi Lambda memiliki kerentanan kode

Kode aplikasi fungsi lambda berisi kerentanan keamanan yang dapat dieksploitasi oleh aktor ancaman. Kerentanan kode termasuk kebocoran data, kelemahan injeksi, enkripsi yang hilang, dan kriptografi lemah yang diidentifikasi melalui analisis kode otomatis. Kerentanan ini menimbulkan risiko keamanan bagi AWS lingkungan Anda, karena penyerang dapat mengeksploitasinya untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Kerentanan kode mewakili kelemahan keamanan yang dapat dirantai bersama dengan vektor serangan lainnya untuk membahayakan fungsi Anda. Mengikuti praktik terbaik keamanan, atasi kerentanan kode ini untuk melindungi fungsi Anda dari serangan.

Remediasi: Perbarui fungsi yang terpengaruh

Tinjau bagian Referensi di tab Kerentanan pada sifat tersebut. Temuan Amazon Inspector mungkin mencakup panduan remediasi khusus dan cuplikan kode yang menunjukkan lokasi kode yang rentan. Atasi masalah keamanan yang teridentifikasi dalam kode fungsi Anda menggunakan blok kode plug-and-play yang disediakan atau dengan menerapkan praktik pengkodean yang aman.

Selalu tinjau saran remediasi kode sebelum mengadopsinya, karena Anda mungkin perlu mengeditnya untuk memastikan kode Anda berfungsi sebagaimana dimaksud. Setelah memperbaiki kerentanan, perbarui kode fungsi Lambda untuk menggunakan versi yang dikoreksi. Untuk petunjuk, lihat Memperbarui kode fungsi di Panduan AWS Lambda Pengembang.

Setelah itu, gunakan versi yang diperbarui. Untuk petunjuk, lihat Menye barkan fungsi Lambda sebagai arsip berkas.zip untuk arsip file.zip atau Membuat fungsi Lambda menggunakan gambar kontainer untuk gambar kontainer. Untuk informasi selengkapnya tentang pemindaian kode Amazon Inspector, lihat Pemindaian kode Amazon Inspector Lambda di Panduan Pengguna Amazon Inspector.

Sifat dampak untuk fungsi Lambda

Sifat dampak menggambarkan radius ledakan potensial dari suatu eksposur. Security Hub menganalisis izin efektif dari prinsipal yang terkait AWS Identity and Access Management dengan fungsi Lambda untuk menentukan sumber daya hilir yang dapat dijangkau penyerang jika fungsinya dikompromikan. Setiap sifat dampak mengidentifikasi pola eskalasi hak istimewa tertentu. Untuk mengurangi radius ledakan Anda, tinjau jalur izin yang dijelaskan di setiap sifat dan hapus hak istimewa yang tidak perlu.

Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa paling sedikit dengan hanya memberikan izin yang diperlukan untuk melakukan tugas. Ganti kebijakan luas dengan kebijakan cakupan yang hanya memberikan tindakan dan sumber daya spesifik yang dibutuhkan. Untuk mengidentifikasi izin yang tidak digunakan untuk dihapus, gunakan Penganalisis Akses IAM untuk menghasilkan rekomendasi berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat Temuan untuk akses eksternal dan tidak digunakan dan M enerapkan izin hak istimewa terkecil di Panduan Pengguna IAM.

Memiliki jalur eksekutor istimewa kontrol penuh

Prinsipal terkait dapat meneruskan peran ke dan menyuntikkan kode ke sumber daya komputasi yang sudah memiliki izin tinggi. Hal ini memungkinkan prinsipal untuk mendapatkan kontrol penuh atas pelaksana dan melakukan tindakan apa pun yang diizinkan oleh peran pelaksana.

Memiliki jalur eskalasi kebijakan langsung

Prinsipal terkait dapat secara langsung memodifikasi kebijakan IAM untuk memberikan izin tambahan kepada dirinya sendiri, meningkatkan hak istimewanya sendiri tanpa sumber daya perantara.

Memiliki jalur pembajakan kebijakan kepercayaan

Prinsipal terkait dapat memodifikasi kebijakan kepercayaan dari peran IAM untuk membiarkan dirinya mengambil peran itu, mendapatkan izin peran tersebut.

Memiliki jalur data ransomware

Prinsipal terkait dapat mengenkripsi atau menghapus data dengan cara yang dapat digunakan untuk ransomware, seperti mengenkripsi objek Amazon S3 dengan kunci yang dikelola pelanggan dan kemudian memodifikasi kebijakan AWS KMS kunci.

Telah menghapus jalur pembatasan

Prinsipal terkait dapat menghapus batasan keamanan seperti batas izin, kebijakan kontrol layanan, atau pernyataan penolakan kebijakan berbasis sumber daya, memperluas apa yang dapat dilakukan oleh prinsipal lain atau sumber daya itu sendiri.

Memiliki jalur pass role buat eksekutor

Prinsipal terkait dapat membuat sumber daya komputasi baru (seperti fungsi Lambda atau instans Amazon EC2) dan memberikannya peran istimewa, secara efektif mencuci izinnya sendiri melalui sumber daya baru.

Memiliki jalur pelaksana peran swap yang ada

Prinsip terkait dapat mengubah peran IAM yang dilampirkan ke sumber daya komputasi yang ada, menggantinya dengan peran yang lebih istimewa untuk meningkatkan akses.

Memiliki jalur eskalasi rantai peran

Prinsipal terkait dapat mengambil urutan peran, di mana setiap peran dalam rantai memiliki izin yang semakin luas, pada akhirnya mencapai peran yang sangat istimewa.

Telah menyuntikkan jalur eksekutor istimewa kode

Prinsip terkait dapat menyuntikkan kode ke sumber daya komputasi yang sedang berjalan yang memiliki izin tinggi, menjalankan operasi arbitrer di bawah peran istimewa sumber daya tersebut.

Telah menonaktifkan jalur jejak audit

Prinsipal terkait dapat menonaktifkan layanan logging atau pemantauan seperti CloudTrail, secara efektif menutupi jejaknya selama atau setelah eskalasi.

Memiliki akses jalur eksekutor yang ada

Prinsipal terkait dapat memanggil atau menghubungkan ke sumber daya komputasi yang ada dan menggunakan peran terlampir untuk melakukan tindakan istimewa.

Memiliki jalur pencetakan kredensi

Prinsipal terkait dapat membuat kredenSIAL jangka panjang baru (seperti kunci akses atau profil login) untuk prinsipal lain, membuat jalur akses persisten yang bertahan dari rotasi kata sandi atau kedaluwarsa sesi.

Memiliki jalur akses data peran pass

Prinsipal terkait dapat membuat sumber daya layanan dan memberikannya peran yang memiliki akses ke data sensitif, mendapatkan akses tidak langsung ke data tersebut melalui sumber daya baru.

Memiliki jalur pembajakan tugas peran lulus

Prinsip terkait dapat meneruskan peran ke tugas yang dijadwalkan atau didorong oleh peristiwa (seperti fungsi Lambda yang dipicu oleh suatu peristiwa), memungkinkannya untuk mengeksekusi kode arbitrer dengan izin peran tersebut.

Memiliki jalur akses data hop tunggal

Prinsipal terkait dapat langsung mengakses sumber daya data sensitif (seperti bucket Amazon S3 atau tabel DynamoDB) melalui izin yang ada, tanpa memerlukan langkah eskalasi menengah.

Memiliki jalur kemajuan kemampuan

Prinsipal terkait memiliki jalur eskalasi hak istimewa yang memajukan kemampuan keseluruhannya melampaui apa yang disarankan oleh izin yang ditetapkan secara langsung. Ini adalah klasifikasi umum untuk jalur yang tidak cocok dengan pola yang lebih spesifik.

Memperbaiki eksposur untuk instans dan cluster Amazon RDS

AWS Security Hub dapat menghasilkan temuan eksposur untuk instans dan cluster Amazon RDS.

Pada konsol Hub Keamanan, instans atau cluster Amazon RDS yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat kesalahan konfigurasi untuk instans dan cluster Amazon RDS
  - Instans Amazon RDS DB dikonfigurasi dengan akses publik

- Cluster Amazon RDS DB memiliki snapshot yang dibagikan secara publik
- Instans Amazon RDS DB memiliki snapshot yang dibagikan secara publik
- Instans Amazon RDS DB memiliki snapshot yang tidak dienkripsi saat diam
- Cluster Amazon RDS DB memiliki snapshot yang tidak dienkripsi saat diam
- Instans Amazon RDS DB memiliki grup keamanan terbuka
- Instans Amazon RDS DB menonaktifkan otentikasi database IAM
- Instans Amazon RDS DB menggunakan nama pengguna admin default
- Cluster Amazon RDS DB menggunakan nama pengguna admin default
- Instans Amazon RDS DB memiliki peningkatan versi minor otomatis yang dinonaktifkan
- Instans Amazon RDS DB menonaktifkan pencadangan otomatis
- Instans Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan
- Cluster Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan
- Instans Amazon RDS DB menggunakan port default untuk mesin database
- Instans Amazon RDS DB tidak tercakup oleh paket cadangan
- Sifat data sensitif untuk instans Amazon RDS DB
  - Instans Amazon RDS DB berisi data sensitif

Sifat kesalahan konfigurasi untuk instans dan cluster Amazon RDS

Berikut ini menjelaskan sifat kesalahan konfigurasi dan langkah-langkah perbaikan untuk instans dan cluster Amazon RDS.

Instans Amazon RDS DB dikonfigurasi dengan akses publik

Instans Amazon RDS dengan akses publik berpotensi dapat diakses melalui internet melalui titik akhir mereka. Meskipun akses publik terkadang diperlukan misalnya fungsionalitas, konfigurasi ini dapat digunakan sebagai vektor serangan potensial bagi pengguna yang tidak sah untuk mencoba mengakses database Anda. Database yang dapat diakses publik dapat terkena pemindaian port, serangan brute force, dan upaya eksploitasi. Mengikuti prinsip-prinsip keamanan standar, batasi paparan publik dari sumber daya database Anda.

Remediasi: Ubah pengaturan akses publik

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka instance DB yang terpengaruh di konsol Amazon RDS. Mengevaluasi apakah instance DB memerlukan aksesibilitas publik

berdasarkan arsitektur aplikasi Anda. Untuk informasi selengkapnya, lihat Menyiapkan akses publik atau pribadi di Amazon RDS.

Cluster Amazon RDS DB memiliki snapshot yang dibagikan secara publik

Snapshot publik dapat diakses oleh siapa pun Akun AWS, yang berpotensi mengekspos data sensitif kepada pengguna yang tidak sah. Setiap Akun AWS orang memiliki izin untuk menyalin snapshot publik ini dan membuat instance DB darinya, yang dapat menyebabkan pelanggaran data atau akses data yang tidak sah. Mengikuti praktik terbaik keamanan, batasi akses ke snapshot Amazon RDS Anda hanya untuk organisasi Akun AWS dan tepercaya.

Remediasi: Konfigurasikan snapshot Amazon RDS untuk akses pribadi

Dalam temuan eksposur, buka sumber daya melalui hyperlink. Untuk informasi tentang cara mengubah pengaturan berbagi snapshot, lihat Berbagi snapshot di Panduan Pengguna Amazon Aurora. Untuk informasi tentang cara menghentikan berbagi snapshot, lihat Mengh entikan berbagi snapshot di Panduan Pengguna Amazon Aurora. .

Instans Amazon RDS DB memiliki snapshot yang dibagikan secara publik

Snapshot publik dapat diakses oleh siapa pun Akun AWS, yang berpotensi mengekspos data sensitif kepada pengguna yang tidak sah. Setiap Akun AWS orang memiliki izin untuk menyalin snapshot publik ini dan membuat instance DB darinya, yang dapat menyebabkan pelanggaran data atau akses data yang tidak sah. Mengikuti praktik terbaik keamanan, batasi akses ke snapshot Amazon RDS Anda hanya untuk organisasi Akun AWS dan tepercaya.

Remediasi: Konfigurasikan snapshot Amazon RDS untuk akses pribadi

Dalam temuan eksposur, buka sumber daya melalui hyperlink. Untuk informasi tentang cara mengubah pengaturan berbagi snapshot, lihat Berbagi snapshot DB di Panduan Pengguna Amazon RDS. Untuk informasi tentang cara menghentikan berbagi snapshot, lihat Ber henti berbagi snapshot DB di Panduan Pengguna Amazon RDS. .

Instans Amazon RDS DB memiliki snapshot yang tidak dienkripsi saat diam

Snapshot instans Amazon RDS DB yang tidak terenkripsi dapat mengekspos data sensitif jika akses tidak sah ke lapisan penyimpanan diperoleh. Tanpa enkripsi, data dalam snapshot berpotensi terekspos melalui akses yang tidak sah. Ini menciptakan risiko pelanggaran data dan pelanggaran kepatuhan. Mengikuti praktik terbaik keamanan, mengenkripsi semua sumber daya database dan cadangannya untuk menjaga kerahasiaan data.

Remediasi: Perbarui sumber daya yang terpengaruh

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka snapshot yang terpengaruh di konsol Amazon RDS. Anda tidak dapat secara langsung mengenkripsi snapshot yang tidak terenkripsi yang ada.

Sebagai gantinya, buat salinan terenkripsi dari snapshot yang tidak dienkripsi. Untuk petunjuk terperinci, lihat Menyalin snapshot cluster DB dan Mengenkripsi sumber daya Amazon RDS di Panduan Pengguna Amazon Aurora.

Cluster Amazon RDS DB memiliki snapshot yang tidak dienkripsi saat diam

Snapshot cluster Amazon RDS DB yang tidak terenkripsi dapat mengekspos data sensitif jika akses tidak sah ke lapisan penyimpanan diperoleh. Tanpa enkripsi, data dalam snapshot berpotensi terekspos melalui akses yang tidak sah. Ini menciptakan risiko pelanggaran data dan pelanggaran kepatuhan. Mengikuti praktik terbaik keamanan, mengenkripsi semua sumber daya database dan cadangannya untuk menjaga kerahasiaan data.

Remediasi: Buat salinan snapshot terenkripsi

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka snapshot yang terpengaruh di konsol Amazon RDS. Anda tidak dapat secara langsung mengenkripsi snapshot yang tidak terenkripsi yang ada.

Sebagai gantinya, buat salinan terenkripsi dari snapshot yang tidak dienkripsi. Untuk petunjuk terperinci, lihat Menyalin snapshot cluster DB dan Mengenkripsi sumber daya Amazon RDS di Panduan Pengguna Amazon Aurora.

Instans Amazon RDS DB memiliki grup keamanan terbuka

Grup keamanan bertindak sebagai firewall virtual untuk instans Amazon RDS Anda untuk mengontrol lalu lintas masuk dan keluar. Grup keamanan terbuka, yang memungkinkan akses tidak terbatas dari alamat IP apa pun, dapat mengekspos instance database Anda ke akses tidak sah dan potensi serangan. Mengikuti prinsip-prinsip keamanan standar, batasi akses grup keamanan ke alamat IP dan port tertentu untuk mempertahankan prinsip hak istimewa terendah.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau aturan grup keamanan dan menilai konfigurasi saat ini

Dalam pencarian eksposur, buka sumber daya untuk Grup Keamanan instans DB. Evaluasi port mana yang terbuka dan dapat diakses dari rentang IP yang luas, seperti`(0.0.0.0/0 or ::/0)`. Untuk informasi tentang melihat detail grup keamanan, lihat DescribeSecurityGroups di Refer ensi API Amazon Elastic Compute Cloud.

Ubah aturan grup keamanan

Ubah aturan grup keamanan Anda untuk membatasi akses ke alamat atau rentang IP tepercaya tertentu. Saat memperbarui aturan grup keamanan Anda, pertimbangkan untuk memisahkan persyaratan akses untuk segmen jaringan yang berbeda dengan membuat aturan untuk setiap rentang IP sumber yang diperlukan atau membatasi akses ke port tertentu. Untuk mengubah aturan grup keamanan, lihat Meng onfigurasi aturan grup keamanan di Panduan Pengguna Amazon EC2. Untuk memodifikasi port default instans database Amazon RDS yang ada, lihat Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon Aurora.

Instans Amazon RDS DB menonaktifkan otentikasi database IAM

Otentikasi basis data IAM memungkinkan Anda untuk mengotentikasi ke database Amazon RDS menggunakan kredentif IAM, bukan kata sandi database. Ini memberikan beberapa manfaat keamanan, seperti manajemen akses terpusat, kredenSIAL sementara, dan penghapusan penyimpanan kata sandi database dalam kode aplikasi. Otentikasi database IAM memungkinkan otentikasi ke instance database dengan token otentikasi alih-alih kata sandi. Akibatnya, lalu lintas jaringan ke dan dari instance database dienkripsi menggunakan SSL. Tanpa otentikasi IAM, database biasanya bergantung pada otentikasi berbasis kata sandi, yang dapat menyebabkan penggunaan kembali kata sandi dan kata sandi yang lemah. Mengikuti praktik terbaik keamanan, aktifkan otentikasi database IAM.

Remediasi: Aktifkan otentikasi database IAM

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka instance DB yang terpengaruh di konsol Amazon RDS. Anda dapat mengaktifkan otentikasi database IAM di opsi Database.

Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan otentikasi basis data IAM di Panduan Pengguna Amazon RDS. Setelah mengaktifkan otentikasi IAM, perbarui instans DB Anda untuk menggunakan otentikasi IAM alih-alih otentikasi berbasis kata sandi.

Instans Amazon RDS DB menggunakan nama pengguna admin default

Menggunakan nama pengguna default (misalnya, “admin”, “root”) untuk instans DB meningkatkan risiko keamanan karena ini dikenal luas dan umumnya ditargetkan dalam serangan brute force. Nama pengguna default dapat diprediksi dan memudahkan pengguna yang tidak berwenang untuk

mencoba mendapatkan akses ke database Anda. Dengan nama pengguna default, penyerang hanya perlu mendapatkan kata sandi daripada membutuhkan keduanya untuk mendapatkan akses ke database Anda. Mengikuti praktik terbaik keamanan, gunakan nama pengguna administrator unik untuk instance database Anda untuk meningkatkan keamanan melalui ketidakjelasan dan mengurangi risiko upaya akses yang tidak sah.

Remediasi: Konfigurasikan nama pengguna administrator yang unik

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka instance DB yang terpengaruh di konsol Amazon RDS. Anda tidak dapat mengubah nama pengguna administrator dari instans Amazon RDS DB yang ada. Untuk membuat nama administrator yang unik, Anda perlu membuat instance DB baru dengan nama pengguna khusus dan memigrasikan data Anda.

Cluster Amazon RDS DB menggunakan nama pengguna admin default

Menggunakan nama pengguna default (misalnya, “admin”, “root”) untuk instans DB meningkatkan risiko keamanan karena ini dikenal luas dan umumnya ditargetkan dalam serangan brute force. Nama pengguna default dapat diprediksi dan memudahkan pengguna yang tidak berwenang untuk mencoba mendapatkan akses ke database Anda. Dengan nama pengguna default, penyerang hanya perlu mendapatkan kata sandi daripada membutuhkan keduanya untuk mendapatkan akses ke database Anda. Mengikuti praktik terbaik keamanan, gunakan nama pengguna administrator unik untuk instance database Anda untuk meningkatkan keamanan melalui ketidakjelasan dan mengurangi risiko upaya akses yang tidak sah.

Remediasi: Konfigurasikan nama pengguna administrator yang unik

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka instance DB yang terpengaruh di konsol Amazon RDS. Anda tidak dapat mengubah nama pengguna administrator dari instans Amazon RDS DB yang ada. Untuk membuat nama administrator yang unik, Anda perlu membuat instance DB baru dengan nama pengguna khusus dan memigrasikan data Anda.

Instans Amazon RDS DB memiliki peningkatan versi minor otomatis yang dinonaktifkan

Peningkatan versi minor otomatis memastikan bahwa instans Amazon RDS Anda secara otomatis menerima peningkatan versi mesin minor saat tersedia. Upgrade ini sering menyertakan patch keamanan penting dan perbaikan bug yang membantu menjaga keamanan dan stabilitas database Anda. Database Anda berisiko berjalan dengan kerentanan keamanan yang diketahui yang telah diperbaiki di versi minor yang lebih baru. Tanpa pembaruan otomatis, instance database dapat mengakumulasi kerentanan keamanan saat CVE baru ditemukan. Mengikuti praktik terbaik keamanan, aktifkan peningkatan versi minor otomatis untuk semua instans Amazon RDS.

Remediasi: Aktifkan peningkatan versi minor otomatis

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka instance DB yang terpengaruh di konsol Amazon RDS. Anda dapat melihat pengaturan peningkatan kecil otomatis di tab Pemeliharaan & pencadangan.

Untuk informasi selengkapnya, lihat Upgrade versi minor otomatis untuk Amazon RDS untuk MySQL. Anda juga dapat mengonfigurasi jendela pemeliharaan agar terjadi selama periode aktivitas database rendah.

Instans Amazon RDS DB menonaktifkan pencadangan otomatis

Pencadangan otomatis menyediakan pemulihan point-in-time untuk instans Amazon RDS Anda, memungkinkan Anda memulihkan database ke titik mana pun dalam periode retensi Anda. Ketika pencadangan otomatis dinonaktifkan, Anda berisiko kehilangan data jika terjadi penghapusan berbahaya, kerusakan data, atau skenario kehilangan data lainnya. Jika terjadi aktivitas berbahaya seperti serangan ransomware, penghapusan tabel database, atau korupsi, kemampuan untuk memulihkan ke titik waktu sebelum insiden mengurangi waktu yang diperlukan untuk pulih dari insiden. Mengikuti praktik terbaik keamanan, aktifkan pencadangan otomatis dengan periode penyimpanan yang sesuai untuk semua database produksi.

Instans Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan

Perlindungan penghapusan database adalah fitur yang membantu mencegah penghapusan instance database Anda. Ketika perlindungan penghapusan dinonaktifkan, database Anda dapat dihapus oleh pengguna mana pun dengan izin yang memadai, yang berpotensi mengakibatkan hilangnya data atau downtime aplikasi. Penyerang dapat menghapus database Anda, yang menyebabkan gangguan layanan, kehilangan data, dan peningkatan waktu pemulihan. Mengikuti praktik terbaik keamanan, aktifkan perlindungan penghapusan untuk instans DB RDS Anda untuk mencegah penghapusan berbahaya.

Remediasi: Aktifkan perlindungan penghapusan untuk cluster Amazon RDS DB Anda

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka cluster DB yang terpengaruh.

Cluster Amazon RDS DB memiliki perlindungan penghapusan dinonaktifkan

Perlindungan penghapusan database adalah fitur yang membantu mencegah penghapusan instance database Anda. Ketika perlindungan penghapusan dinonaktifkan, database Anda dapat dihapus oleh pengguna mana pun dengan izin yang memadai, yang berpotensi mengakibatkan hilangnya data atau downtime aplikasi. Penyerang dapat menghapus database Anda, yang menyebabkan gangguan

layanan, kehilangan data, dan peningkatan waktu pemulihan. Mengikuti praktik terbaik keamanan, aktifkan perlindungan penghapusan untuk cluster DB RDS Anda untuk mencegah penghapusan berbahaya.

Remediasi: Aktifkan perlindungan penghapusan untuk cluster Amazon RDS DB Anda

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka cluster DB yang terpengaruh.

Instans Amazon RDS DB menggunakan port default untuk mesin database

Instans Amazon RDS yang menggunakan port default untuk mesin database mungkin menghadapi peningkatan risiko keamanan, karena port default ini dikenal luas dan sering ditargetkan oleh alat pemindaian otomatis. Memodifikasi instance DB Anda untuk menggunakan port non-default menambahkan lapisan keamanan tambahan melalui ketidakjelasan, sehingga lebih sulit bagi pengguna yang tidak berwenang untuk melakukan serangan otomatis atau tertarget pada database Anda. Port default biasanya dipindai oleh orang yang tidak berwenang, dan dapat menyebabkan instans DB Anda ditargetkan. Mengikuti praktik terbaik keamanan, ubah port default ke port khusus untuk mengurangi risiko serangan otomatis atau tertarget.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Perbarui sumber daya yang terpengaruh

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka instance DB yang terpengaruh di konsol Amazon RDS.

Perbarui string koneksi aplikasi

Setelah mengubah port, perbarui semua aplikasi dan layanan yang terhubung ke instance Amazon RDS Anda untuk menggunakan nomor port baru.

Instans Amazon RDS DB tidak tercakup oleh paket cadangan

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Jika instans DB Anda tidak tercakup oleh paket cadangan, Anda berisiko kehilangan data jika terjadi penghapusan berbahaya, kerusakan data, atau skenario kehilangan data lainnya. Jika terjadi aktivitas berbahaya seperti serangan ransomware, penghapusan tabel database, atau korupsi, kemampuan untuk memulihkan ke titik waktu sebelum insiden mengurangi waktu yang diperlukan untuk pulih dari insiden. Mengikuti praktik

terbaik keamanan, sertakan instans Amazon RDS Anda dalam rencana cadangan untuk memastikan perlindungan data.

Remediasi: Membuat dan menetapkan rencana cadangan untuk instans DB Anda

Dalam temuan eksposur, pilih tautan sumber daya. Ini membuka instance DB yang terpengaruh di konsol Amazon RDS. Pertimbangkan frekuensi pencadangan, periode retensi, dan aturan siklus hidup yang terbaik untuk aplikasi Anda.

Sifat data sensitif untuk instans Amazon RDS DB

Berikut adalah ciri-ciri data sensitif untuk instans Amazon RDS DB dan langkah-langkah perbaikan yang disarankan.

Instans Amazon RDS DB berisi data sensitif

Pemindaian keamanan data telah mengkonfirmasi bahwa catatan sensitif ada di instans Amazon RDS DB. Produk keamanan data terintegrasi menetapkan sifat ini ketika memeriksa konten instance DB dan mengidentifikasi catatan yang memerlukan perlindungan.

Kehadiran data sensitif meningkatkan dampak dari setiap kelemahan lainnya pada instance DB yang sama. Jalur jaringan atau konfigurasi akses permisif yang sebaliknya akan mengekspos data aplikasi malah mengekspos catatan yang diatur atau rahasia. Aktor ancaman yang mencapai instans DB dapat menanyakan dan menyalin catatan tersebut secara massal dan menyimpannya di luar lingkungan Anda. Aktor ancaman juga dapat menggunakan kredenSIAL yang dipulihkan untuk mengotentikasi ke sistem lain. Mengikuti praktik terbaik keamanan, sebaiknya batasi akses jaringan dan identitas ke instans Amazon RDS DB yang menyimpan catatan sensitif, dan mengenkripsi catatan tersebut saat istirahat dan dalam perjalanan.

Data sensitif dapat mencakup:

- KredenSIAL — seperti kata sandi, kunci akses, dan string koneksi
- Informasi pengenal pribadi
- Informasi keuangan — seperti nomor rekening dan data kartu pembayaran
- Konten rahasia yang membutuhkan perlindungan

Menghapus catatan sensitif adalah satu-satunya cara untuk menghapus sifat ini. Jika beban kerja Anda memerlukan instance DB untuk menyimpan data sensitif, praktik terbaik keamanan berikut mengurangi risiko paparan.

Tinjau data sensitif pada instance DB

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini membuka instance DB yang terpengaruh. Perhatikan pengidentifikasi instans DB, dan catat grup keamanan VPC yang tercantum di bawah Konek tivitas & keamanan. Tinjau temuan keamanan data yang melaporkan catatan sensitif untuk menentukan database, skema, dan tabel mana yang berisi data tersebut.

Berdasarkan jenis data sensitif yang ditemukan, terapkan kontrol keamanan yang sesuai:

- Batasi akses jaringan masuk — Di konsol Amazon RDS, pilih Database, pilih instance DB, dan pilih Konek tivitas & keamanan. Buka setiap grup keamanan VPC terlampir dan tinjau aturan inbound-nya. Ganti aturan apa pun yang mengizinkan port database dari `0.0.0.0/0` atau `::/0` dengan rentang CIDR tertentu atau ID grup keamanan yang digunakan aplikasi Anda. Untuk informasi selengkapnya, lihat Mengontrol akses dengan grup keamanan di Panduan Pengguna Amazon RDS.
- Hapus aksesibilitas publik — Di konsol Amazon RDS, pilih instance DB, pilih Ubah, dan di bawah Konek tivitas setel Ak ses publik ke Tidak dapat diakses publik. Tempatkan instance DB di subnet pribadi yang tidak memiliki rute ke gateway internet. Jangkau dari aplikasi Anda melalui VPC, AWS Direct Connect, atau koneksi VPN. Untuk informasi selengkapnya, lihat Bek erja dengan instance DB di VPC di Panduan Pengguna Amazon RDS.
- Batasi siapa yang dapat mengotentikasi ke database — Berikan setiap aplikasi dan pengguna hanya hak istimewa database yang diperlukan untuk fungsinya. Cabut akses baca ke tabel yang berisi catatan sensitif dari pengguna database mana pun yang tidak membutuhkannya. Gunakan otentikasi database IAM sehingga identitas IAM dan token berumur pendek mengontrol akses alih-alih kata sandi basis data yang berumur panjang. Untuk informasi selengkapnya, lihat otentikasi database IAM di Panduan Pengguna Amazon RDS.
- Enkripsi catatan sensitif saat diam — Di konsol Amazon RDS, pilih instance DB dan pilih tab Konfigurasi untuk melihat apakah instance DB menggunakan enkripsi. Anda tidak dapat mengaktifkan enkripsi saat diam pada instans DB yang tidak terenkripsi yang ada. Untuk mengenkripsi datanya, buat snapshot dari instance DB. Salin snapshot dan pilih kunci AWS KMS untuk salinannya, lalu kembalikan salinan snapshot terenkripsi ke instance DB baru. Arahkan ulang aplikasi Anda di titik akhir baru, dan hapus instans DB yang tidak terenkripsi dan snapshot-nya. Untuk informasi selengkapnya, lihat Mengenkripsi sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.
- Memerlukan enkripsi saat transit — Konfigurasikan klien database Anda untuk terhubung SSL/TLS menggunakan bundel sertifikat Amazon RDS. Menerapkan koneksi terenkripsi pada instance DB melalui parameter yang disediakan mesin database Anda untuk tujuan itu. Untuk informasi

selengkapnya, lihat Menggunakan SSL/TLS untuk mengenkripsi koneksi ke instans atau cluster DB di Panduan Pengguna Amazon RDS.

- Memantau akses ke instance DB — Publikasikan log mesin database ke Amazon Log CloudWatch s, dan tinjau koneksi dari sumber yang tidak terduga dan untuk kueri terhadap tabel yang berisi catatan sensitif. Untuk informasi selengkapnya, lihat Memantau file log Amazon RDS di Panduan Pengguna Amazon RDS.

Memperbaiki eksposur untuk bucket Amazon S3

AWS Security Hub dapat menghasilkan temuan eksposur untuk bucket Amazon Simple Storage Service (Amazon S3).

Di konsol Hub Keamanan, bucket Amazon S3 yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber Daya pada detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat kesalahan konfigurasi untuk bucket Amazon S3
  - Bucket Amazon S3 memiliki versi yang dinonaktifkan
  - Bucket Amazon S3 memiliki Object Lock dinonaktifkan

  - Bucket Amazon S3 tidak dienkripsi saat diam dengan AWS KMS keys
  - Multi-factor Penghapusan otentikasi (MFA) dinonaktifkan pada bucket Amazon S3 berversi
  - Bucket Amazon S3 memungkinkan prinsipal dari yang lain AWS akun untuk memodifikasi izin bucket
- Sifat jangkauan untuk bucket Amazon S3
  - Bucket Amazon S3 memiliki akses baca publik
  - Bucket Amazon S3 memiliki akses tulis publik
- Sifat data sensitif untuk bucket Amazon S3
  - Bucket Amazon S3 berisi data sensitif

Sifat kesalahan konfigurasi untuk bucket Amazon S3

Berikut adalah sifat kesalahan konfigurasi untuk bucket Amazon S3 dan langkah-langkah remediasi yang disarankan.

Bucket Amazon S3 memiliki versi yang dinonaktifkan

Amazon S3 Versioning membantu Anda menyimpan beberapa varian objek dalam bucket yang sama. Saat pembuatan versi dinonaktifkan, Amazon S3 hanya menyimpan versi terbaru dari setiap objek, yang berarti bahwa jika objek dihapus atau diganti secara tidak sengaja atau jahat, objek tersebut tidak dapat dipulihkan. Versioning-enabled bucket memberikan perlindungan terhadap penghapusan yang tidak disengaja, kegagalan aplikasi, dan insiden keamanan seperti serangan ransomware, di mana modifikasi atau penghapusan data yang tidak sah dapat terjadi. Mengikuti praktik terbaik keamanan, aktifkan pembuatan versi untuk bucket yang berisi data penting yang akan sulit atau tidak mungkin dibuat ulang jika hilang.

Remediasi: Aktifkan pembuatan versi

Untuk mengaktifkan Pembuatan Versi Amazon S3 pada bucket, lihat Meng aktifkan pembuatan versi pada bucket di Panduan Pengguna Amazon S3. Saat mengaktifkan pembuatan versi, pertimbangkan untuk menerapkan aturan siklus hidup untuk mengelola penyimpanan, karena pembuatan versi akan mempertahankan beberapa salinan objek.

Bucket Amazon S3 memiliki Object Lock dinonaktifkan

Amazon S3 Object Lock menyediakan model write-once-read-many (WORM) untuk objek Amazon S3, mencegahnya dihapus atau diganti untuk jangka waktu tertentu atau tanpa batas waktu. Ketika Object Lock dinonaktifkan, objek Anda mungkin rentan terhadap penghapusan, modifikasi, atau

enkripsi yang tidak disengaja atau berbahaya oleh ransomware. Object Lock sangat penting untuk kepatuhan terhadap persyaratan peraturan yang menuntut penyimpanan data yang tidak dapat diubah dan untuk perlindungan terhadap ancaman canggih seperti ransomware yang mungkin mencoba mengenkripsi data Anda. Dengan mengaktifkan Object Lock, Anda dapat menerapkan kebijakan retensi sebagai lapisan perlindungan data tambahan dan membuat strategi pencadangan yang tidak dapat diubah untuk data penting Anda. Mengikuti praktik terbaik keamanan, aktifkan Object Lock untuk mencegah modifikasi berbahaya pada objek Anda.

Remediasi: Konfigurasikan Kunci Objek S3

Perhatikan bahwa Object Lock hanya dapat diaktifkan saat membuat bucket baru, jadi Anda perlu membuat bucket baru dengan Object Lock diaktifkan. Untuk migrasi besar, pertimbangkan untuk menggunakan Operasi Batch untuk menyalin objek ke bucket baru. Sebelum mengunci objek apa pun, Anda juga harus mengaktifkan Amazon S3 Versioning dan Object Lock pada bucket. Karena Object Lock hanya dapat diaktifkan pada bucket baru, Anda harus memigrasikan data yang ada ke bucket baru dengan Object Lock diaktifkan. Untuk informasi tentang cara mengonfigurasi Object Lock pada bucket, lihat Mengon figurasi Kunci Objek Amazon S3 di Panduan Pengguna Amazon S3. Setelah mengatur Object Lock, pilih mode retensi yang sesuai sesuai dengan lingkungan Anda.

Bucket Amazon S3 tidak dienkripsi saat diam dengan AWS KMS keys

Amazon S3 menerapkan enkripsi sisi server dengan kunci terkelola Amazon S3 sebagai tingkat enkripsi default untuk semua bucket baru. Meskipun kunci terkelola Amazon S3 memberikan perlindungan enkripsi yang kuat, kunci tersebut tidak menawarkan tingkat kontrol akses dan kemampuan audit yang sama dengan AWS Key Management Service kunci. Saat menggunakan kunci KMS, akses ke objek memerlukan izin ke bucket Amazon S3 dan kunci KMS yang mengenkripsi objek. Hal ini sangat penting untuk data sensitif di mana Anda memerlukan kontrol terperinci atas siapa yang dapat mengakses objek terenkripsi dan pencatatan audit komprehensif penggunaan kunci enkripsi. Mengikuti praktik terbaik keamanan, gunakan kunci KMS untuk mengenkripsi bucket yang berisi data sensitif atau untuk lingkungan dengan persyaratan kepatuhan yang ketat.

Remediasi: Konfigurasikan kunci bucket S3

Untuk mengonfigurasi bucket agar menggunakan kunci bucket Amazon S3 untuk objek baru, lihat Mengon figurasi bucket Anda untuk menggunakan Kunci Amazon S3 Bucket with SSE-KMS untuk objek baru di Panduan Pengguna Amazon S3. Untuk informasi tentang cara mengenkripsi objek yang ada, lihat Mengen kripsi objek dengan Operasi Batch Amazon S3 di Blog Peny AWS impanan.

Saat menerapkan AWS KMS enkripsi, pertimbangkan hal berikut:

- Manajemen kunci — Memutuskan apakah akan menggunakan kunci ter AWS kelola atau kunci yang dikelola pelanggan (CMK). CMK menawarkan pelanggan kontrol penuh atas siklus hidup dan penggunaan kunci mereka. Untuk informasi selengkapnya tentang perbedaan antara kedua jenis kunci ini, lihat kunci AWS KMS di Panduan Peng AWS Key Management Service embang.
- Rotasi kunci — Untuk langkah-langkah keamanan tambahan, aktifkan rotasi kunci otomatis untuk kunci KMS Anda. Untuk informasi selengkapnya, lihat Mengaktifkan rotasi tombol otomatis di Panduan AWS Key Management Service Pengembang.

Multi-factor Penghapusan otentikasi (MFA) dinonaktifkan pada bucket Amazon S3 berversi

Multi-factor Hapus otentikasi (MFA) menyediakan lapisan keamanan tambahan untuk bucket Amazon S3 Anda. Ini membutuhkan otentikasi multi-faktor untuk operasi Amazon S3 yang merusak. Ketika penghapusan MFA dinonaktifkan, pengguna dengan izin yang sesuai dapat menghapus versi objek secara permanen atau menangguhkan pembuatan versi pada bucket Anda tanpa tantangan otentikasi tambahan. Mengaktifkan penghapusan MFA membantu melindungi dari penghapusan data yang tidak sah atau tidak disengaja, memberikan perlindungan yang ditingkatkan terhadap serangan ransomware, ancaman orang dalam, dan kesalahan operasional. Penghapusan MFA sangat berharga untuk bucket yang berisi data penting atau peka terhadap kepatuhan yang harus dilindungi dari penghapusan yang tidak sah. Mengikuti praktik terbaik keamanan, aktifkan MFA untuk bucket Amazon S3 Anda.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau jenis MFA

AWS mendukung jenis https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html#id_credentials_mfa-types MFA berikut. Meskipun otentikasi dengan perangkat fisik biasanya memberikan perlindungan keamanan yang lebih ketat, menggunakan semua jenis MFA lebih aman daripada menonaktifkan MFA.

Menerapkan MFA di tingkat kebijakan sumber daya

Gunakan kunci `aws:MultiFactorAuthAge` kondisi dalam kebijakan bucket untuk mewajibkan MFA untuk operasi sensitif. Untuk informasi selengkapnya, lihat Memerlukan MFA di Panduan Pengguna Amazon S3.

Aktifkan MFA

Untuk mengaktifkan penghapusan MFA, pertama-tama, pastikan pembuatan versi diaktifkan di bucket Amazon S3 Anda. Penghapusan MFA hanya didukung pada bucket yang mengaktifkan pembuatan versi. Untuk informasi tentang cara mengaktifkan pembuatan versi Amazon S3, lihat Meng aktifkan pembuatan versi pada bucket di Panduan Pengguna Amazon S3. Penghapusan MFA tidak dapat diaktifkan melalui konsol Amazon S3. Anda harus menggunakan Amazon S3 API atau AWS CLI. Untuk informasi selengkapnya, lihat Meng onfigurasi penghap usan MFA di Panduan Pengguna Amazon S3.

Bucket Amazon S3 memungkinkan prinsipal dari yang lain AWS akun untuk memodifikasi izin bucket

Kebijakan bucket Amazon S3 mengontrol akses ke bucket dan objek. Ketika kebijakan bucket mengizinkan prinsipal dari AWS akun lain untuk mengubah izin bucket, pengguna yang tidak sah dapat mengonfigurasi ulang bucket Anda. Jika kredentif utama eksternal dikompromikan, pengguna yang tidak sah dapat memperoleh kendali atas bucket Anda, yang menyebabkan pelanggaran data atau gangguan layanan. Mengikuti prinsip-prinsip keamanan standar, batasi tindakan pengelolaan izin hanya untuk prinsipal tepercaya.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Meninjau dan mengidentifikasi kebijakan bucket

Dalam eksposur, identifikasi bucket Amazon S3 di bidang ARN. Di konsol Amazon S3, pilih bucket, dan arahkan ke tab Izin untuk meninjau kebijakan bucket. Tinjau kebijakan izin yang dilampirkan ke bucket. Cari pernyataan kebijakan yang memberikan tindakan seperti `s3:PutBucketPolicy`, `s3:PutBucketAcl`, `s3:DeleteBucketPolicy`, `s3:*` atau pernyataan kebijakan yang memungkinkan akses ke prinsipal di luar akun Anda, seperti yang ditunjukkan dalam pernyataan utama.

Ubah kebijakan bucket

Ubah kebijakan bucket untuk menghapus atau membatasi tindakan yang diberikan ke AWS akun lain:

- Hapus pernyataan kebijakan yang memberikan tindakan pengelolaan izin akun eksternal.
- Jika akses lintas akun diperlukan, ganti izin luas (`s3:*`) dengan tindakan tertentu yang tidak menyertakan manajemen izin bucket.

Untuk informasi tentang memodifikasi kebijakan bucket, lihat Men ambahkan kebijakan bucket dengan menggunakan konsol Amazon S3 di Panduan Pengguna Amazon S3.

Sifat jangkauan untuk bucket Amazon S3

Berikut adalah ciri-ciri keterjangkauan untuk bucket Amazon S3 dan langkah-langkah remediasi yang disarankan.

Bucket Amazon S3 memiliki akses baca publik

Bucket Amazon S3 dengan akses baca publik memungkinkan siapa saja di internet untuk melihat isi bucket Anda. Meskipun ini mungkin diperlukan untuk situs web yang dapat diakses publik atau sumber daya bersama, hal ini dapat menciptakan risiko keamanan jika bucket berisi data sensitif. Akses baca publik dapat menyebabkan tampilan dan pengunduhan yang tidak sah, yang dapat menyebabkan pelanggaran data jika data sensitif disimpan dalam bucket tersebut. Mengikuti prinsip keamanan standar, batasi akses ke bucket Amazon S3 untuk pengguna dan sistem yang diperlukan.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Blokir akses publik di tingkat bucket

Amazon S3 menyediakan setelan Blok Akses Publik yang dapat dikonfigurasi di tingkat bucket dan akun untuk mencegah akses publik terlepas dari kebijakan bucket atau ACL. Untuk informasi selengkapnya, lihat Mem blokir akses publik ke penyimpanan Amazon S3 Anda di Panduan Pengguna Amazon S3. Setelah memblokir akses publik, tinjau konfigurasi kontrol akses bucket Anda untuk memastikannya selaras dengan persyaratan akses Anda. Kemudian tinjau kebijakan bucket Amazon S3 Anda untuk secara eksplisit menentukan siapa yang dapat mengakses bucket Anda. Untuk contoh kebijakan bucket, lihat Contoh kebijakan bucket Amazon S3 di Panduan Pengguna Amazon S3.

Metode akses alternatif

Jika akses baca publik diperlukan, pertimbangkan alternatif yang lebih aman ini:

- Amazon CloudFront — Gunakan CloudFront dengan Origin Access Identity (OAI) atau Origin Access Control (OAC) untuk mengizinkan akses baca dari bucket Amazon S3 pribadi. Alternatif ini membatasi akses langsung ke bucket Amazon S3 Anda sambil memungkinkan konten dapat diakses publik melalui CloudFront. Untuk informasi selengkapnya, lihat Membatasi akses ke sumber Amazon S3 di Panduan CloudFront Pengembang Amazon.
- URL yang ditandatangani sebelumnya — Gunakan URL yang ditandatangani sebelumnya untuk akses sementara ke objek tertentu. Untuk informasi selengkapnya, lihat Berbagi objek dengan URL yang telah ditandatangani sebelumnya di Panduan Pengguna Amazon S3.

Bucket Amazon S3 memiliki akses tulis publik

Bucket Amazon S3 dengan akses tulis publik memungkinkan siapa pun di internet untuk mengunggah, memodifikasi, atau menghapus objek di bucket Anda. Ini menciptakan risiko keamanan yang signifikan, termasuk potensi seseorang untuk mengunggah file berbahaya, memodifikasi file yang ada, dan menghapus data. Akses tulis publik menciptakan kerentanan keamanan yang dapat dieksploitasi oleh penyerang. Mengikuti prinsip keamanan standar, batasi akses tulis ke bucket Amazon S3 Anda hanya untuk pengguna dan sistem yang diperlukan.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Memblokir akses publik di tingkat akun dan bucket

Amazon S3 menyediakan setelan akses publik blok yang dapat dikonfigurasi di tingkat bucket dan akun untuk mencegah akses publik terlepas dari kebijakan bucket atau ACL. Untuk informasi selengkapnya, lihat Mem blokir akses publik ke penyimpanan Amazon S3 Anda di Panduan Pengguna Amazon S3.

Ubah kebijakan bucket

Untuk pendekatan yang lebih terperinci untuk menghapus akses tulis publik, tinjau kebijakan bucket. Anda dapat mencari `s3:PutObject`,`s3:DeleteObject`, atau `s3:*`. Untuk informasi selengkapnya tentang mengelola kebijakan bucket, lihat Kebijakan Bucket untuk Amazon S3 di Panduan Pengguna Amazon S3.

Metode akses alternatif

Jika akses tulis publik diperlukan, pertimbangkan alternatif yang lebih aman ini:

- URL yang ditandatangani sebelumnya — Gunakan URL yang ditandatangani sebelumnya untuk akses sementara ke objek tertentu. Untuk informasi selengkapnya, lihat Berbagi objek dengan URL yang telah ditandatangani sebelumnya di Panduan Pengguna Amazon S3.
- Proksi Amazon API Gateway — Gunakan perantara seperti API Gateway with AWS Lambda untuk memvalidasi dan mengotorisasi permintaan sebelum menulis ke bucket Amazon S3 Anda. Pendekatan ini memastikan bahwa klien tidak pernah menulis ke bucket secara langsung. Untuk informasi selengkapnya, lihat Tutorial: Membuat REST API sebagai proxy Amazon S3 di Panduan Pengembang API Gateway.
- Amazon CloudFront — Gunakan CloudFront dengan Origin Access Control (OAC) yang dikonfigurasi untuk selalu menandatangani permintaan. Aktifkan metode PUT dan POST untuk

mengizinkan penulisan yang diautentikasi tanpa mengekspos bucket Amazon S3 Anda secara langsung. Konfigurasikan kebijakan bucket Anda untuk membatasi `s3:DeleteObject` izin hanya pada prinsipal resmi, sehingga pengguna yang tidak sah tidak dapat menghapus objek yang ingin Anda simpan. Untuk informasi selengkapnya, lihat Mem batasi akses ke sumber Amazon S3 di Panduan CloudFront Pengembang Amazon.

Sifat data sensitif untuk bucket Amazon S3

Berikut adalah ciri-ciri data sensitif untuk bucket Amazon S3 dan langkah-langkah remediasi yang disarankan.

Bucket Amazon S3 berisi data sensitif

Pemindaian keamanan data telah mengkonfirmasi bahwa data sensitif ada di bucket Amazon S3. Produk keamanan data terintegrasi menetapkan sifat ini ketika memeriksa objek dalam bucket dan mengidentifikasi konten yang memerlukan perlindungan. Security Hub melaporkan sifat dengan cara yang sama terlepas dari produk mana yang melakukan inspeksi.

Data sensitif dapat mencakup:

- Kredensial
- Informasi pengenal pribadi
- Informasi keuangan
- Konten rahasia yang membutuhkan perlindungan

Jika data sensitif terekspos melalui kesalahan konfigurasi atau akses yang tidak sah, hal itu dapat menyebabkan pelanggaran kepatuhan, pelanggaran data, pencurian identitas, atau kerugian finansial. Mengikuti praktik terbaik keamanan, pastikan klasifikasi data yang tepat dan pemantauan terus menerus terhadap data sensitif di bucket Amazon S3 Anda.

Remediasi

Untuk menghapus sifat ini, hapus data sensitif dari bucket. Jika beban kerja Anda memerlukan bucket untuk menyimpan data sensitif, terapkan kontrol keamanan berikut untuk mengurangi risiko paparan.

Tinjau data sensitif dalam bucket

Dalam temuan eksposur, pilih Buka sumber daya. Tinjau temuan keamanan data yang melaporkan data sensitif untuk menentukan objek atau awalan mana yang mengandungnya. Jika deteksi berasal

dari Macie, jenis temuan menggambarkan kategori data sensitif. Untuk informasi selengkapnya, lihat Jenis temuan Macie di Panduan Pengguna Amazon Macie.

Berdasarkan jenis data sensitif yang ditemukan, terapkan kontrol keamanan yang sesuai:

- Batasi akses ke bucket — Tinjau izin bucket untuk memastikannya mengikuti prinsip hak istimewa terendah. Gunakan kebijakan IAM, kebijakan bucket, dan ACL untuk membatasi akses. Untuk informasi selengkapnya, lihat Manajemen Identitas dan Akses untuk Amazon S3 di Panduan Pengguna Amazon S3.
- Aktifkan enkripsi sisi server — Aktifkan enkripsi sisi server dengan kunci KMS untuk perlindungan tambahan. Untuk informasi selengkapnya, lihat Menggunakan enkripsi sisi server dengan kunci AWS KMS (SSE-KMS) di Panduan Pengguna Amazon S3.
- Menyunting atau mengubah data sensitif — Jika objek tidak perlu mempertahankan nilai sensitif, gunakan AWS Glue DataBrew untuk menyiapkan data. Terapkan transformasi masking, penggantian, atau hashing yang menghapus nilai-nilai tersebut sebelum sistem hilir mengkonsumsi data. Tulis output yang disiapkan ke bucket terpisah yang memiliki kontrol aksesnya sendiri. Untuk informasi selengkapnya, lihat Apa yang AWS Glue DataBrew ada di Panduan AWS Glue DataBrew Pengembang.

Memperbaiki eksposur untuk instans SageMaker notebook Amazon

AWS Security Hub dapat menghasilkan temuan eksposur untuk inst SageMaker ans notebook Amazon.

Pada konsol Hub Keamanan, instance notebook yang terlibat dalam penemuan eksposur dan informasi pengidentifikasinya tercantum di bagian Resources dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan

menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang diberikan dalam topik ini mungkin memerlukan konsultasi tambahan di AWS sumber daya lain.

Daftar Isi

- Sifat kesalahan konfigurasi untuk instans SageMaker notebook Amazon
  - Instans SageMaker notebook Amazon mengaktifkan akses internet langsung
  - Instans SageMaker notebook Amazon mengaktifkan akses root
- Sifat data sensitif untuk inst SageMaker ans notebook Amazon
  - Instans SageMaker notebook Amazon berisi data sensitif
- Ciri-ciri dampak untuk inst SageMaker ans notebook Amazon
  - Memiliki jalur eksekutor istimewa kontrol penuh
  - Memiliki jalur eskalasi kebijakan langsung
  - Memiliki jalur pembajakan kebijakan kepercayaan
  - Memiliki jalur data ransomware
  - Telah menghapus jalur pembatasan
  - Memiliki jalur pass role buat eksekutor
  - Memiliki jalur pelaksana peran swap yang ada
  - Memiliki jalur eskalasi rantai peran
  - Telah menyuntikkan jalur eksekutor istimewa kode
  - Telah menonaktifkan jalur jejak audit
  - Memiliki akses jalur eksekutor yang ada
  - Memiliki jalur pencetakan kredensi
  - Memiliki jalur akses data peran pass
  - Memiliki jalur pembajakan tugas peran lulus
  - Memiliki jalur akses data hop tunggal
  - Memiliki jalur kemajuan kemampuan

Sifat kesalahan konfigurasi untuk instans SageMaker notebook Amazon

Berikut adalah ciri-ciri kesalahan konfigurasi untuk instans SageMaker notebook Amazon dan langkah-langkah perbaikan yang disarankan.

Instans SageMaker notebook Amazon mengaktifkan akses internet langsung

Ketika `DirectInternetAccess` diaktifkan pada instance SageMaker notebook Amazon, lalu lintas keluar dialihkan melalui gateway terjemahan alamat SageMaker-managed jaringan (NAT) ke internet. Ini menyediakan jalur keluar yang dapat digunakan untuk eksfiltrasi data atau sebagai saluran perintah-dan-kontrol jika notebook disusupi. Mengikuti praktik terbaik keamanan, nonaktifkan akses internet langsung dan tempatkan instance notebook di VPC dengan titik akhir VPC untuk layanan yang diperlukan. AWS

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Nonaktifkan akses internet langsung

Peng `DirectInternetAccess` aturan tidak dapat diubah setelah instance buku catatan dibuat. Untuk menonaktifkannya, buat instance notebook baru dengan dis `DirectInternetAccess` etel ke `Disabled` dalam subnet pribadi dalam VPC, lalu migrasikan buku catatan dan data Anda dari instance yang ada. Untuk petunjuk, lihat Men yambungkan instance notebook di VPC ke sumber daya eksternal di Panduan SageMaker Pengembang Amazon.

Konfigurasikan titik akhir VPC

Saat akses internet langsung dinonaktifkan, instance notebook memerlukan titik akhir VPC untuk mengakses AWS layanan seperti Amazon S3 dan Amazon SageMaker API. Buat titik akhir VPC antarmuka untuk layanan yang dibutuhkan notebook Anda. Untuk informasi tentang titik akhir VPC, lihat Apa itu? AWS PrivateLink dalam AWS PrivateLink panduan.

Instans SageMaker notebook Amazon mengaktifkan akses root

Saat `RootAccess` diaktifkan pada instance SageMaker notebook Amazon, pengguna memiliki hak akses OS-level root penuh. Akses root memungkinkan modifikasi sistem sewenang-wenang, pintu belakang yang persisten, dan instalasi paket tidak terbatas. Mengikuti praktik terbaik keamanan, nonaktifkan akses root untuk instance notebook kecuali jika diperlukan secara eksplisit untuk alur kerja Anda.

Remediasi: Nonaktifkan akses root

Anda tidak dapat mengubah `RootAccess` pengaturan pada instance notebook yang sedang berjalan. Untuk menonaktifkannya, hentikan instance, lalu perbarui konfigurasi instans untuk diset `RootAccess` elDisabled. Sebagian besar alur kerja notebook, termasuk menginstal paket dengan `pip` dan menjalankan konfigurasi siklus hidup, terus bekerja tanpa akses root. Untuk petunjuk, lihat Mengontrol akses root ke instance SageMaker notebook Amazon di Panduan SageMaker Pengembang Amazon.

Pertimbangan tambahan

Jika akses root diperlukan untuk tugas tertentu, pertimbangkan untuk menggunakan buku catatan Amazon SageMaker Studio sebagai gantinya, yang menyediakan lingkungan berbasis wadah terisolasi dengan kontrol akses yang lebih terperinci. Anda juga dapat menggunakan konfigurasi siklus hidup untuk melakukan pra-instal paket yang diperlukan pada waktu pembuatan instance, sehingga mengurangi kebutuhan akan akses root selama penggunaan normal.

Sifat data sensitif untuk inst SageMaker ans notebook Amazon

Berikut adalah ciri-ciri data sensitif untuk instans SageMaker notebook Amazon dan langkah-langkah perbaikan yang disarankan.

Instans SageMaker notebook Amazon berisi data sensitif

Pemindaian keamanan data telah mengkonfirmasi bahwa data sensitif ada di instance SageMaker notebook Amazon. Produk keamanan data terintegrasi menetapkan sifat ini. Produk memeriksa file notebook, output, dan penyimpanan terlampir, dan mengidentifikasi konten yang memerlukan perlindungan. Kami melaporkan sifat ini di Security Hub secara konsisten, terlepas dari produk terintegrasi mana yang melakukan inspeksi.

Data sensitif meningkatkan dampak dari setiap kelemahan lainnya pada instance notebook yang sama. Peran eksekusi permisif, jalur keluar internet langsung, atau akses yang terlalu luas mengekspos konten yang diatur atau rahasia. Aktor ancaman yang mencapai notebook dapat membaca dan menyalin catatan tersebut dari file notebook, sel keluaran, dan pos pemeriksaan yang disimpan. Aktor ancaman kemudian dapat menyimpan catatan tersebut di luar lingkungan Anda. Mereka juga dapat menggunakan kredenSIAL apa pun yang ditemukan di notebook untuk mengotentikasi ke sistem lain.

Mengikuti praktik terbaik keamanan, sebaiknya batasi akses ke instans notebook yang menyimpan data sensitif, dan mengenkripsi penyimpanan terlampir saat diam.

Data sensitif dapat mencakup:

- KredenSIAL — seperti kata sandi, kunci akses, dan string koneksi
- Informasi pengenal pribadi
- Informasi keuangan — seperti nomor rekening dan data kartu pembayaran
- Konten rahasia yang membutuhkan perlindungan

Menghapus data sensitif dari notebook adalah satu-satunya cara untuk menghapus sifat ini. Jika notebook harus mereferensikan data sensitif, praktik terbaik keamanan berikut mengurangi risiko paparan.

Meninjau data sensitif pada instance notebook

Dalam temuan eksposur, buka sumber daya dengan hyperlink. Ini membuka instance notebook yang terpengaruh. Perhatikan nama instance buku catatan, AWS akun, dan Wil AWS ayah. Tinjau temuan keamanan data yang melaporkan data sensitif untuk menentukan file notebook, sel keluaran, atau pos pemeriksaan mana yang berisi data tersebut.

Berdasarkan jenis data sensitif yang ditemukan, terapkan kontrol keamanan yang sesuai:

- Hapus nilai sensitif dari buku catatan — Hapus nilai sensitif dari kode buku catatan dan hapus sel keluaran yang berisi nilai tersebut. Hapus setiap pos pemeriksaan yang disimpan dan salinan yang diekspor yang mempertahankan nilai. Jika nilai harus tetap direferensikan, gantilah dengan placeholder token atau bertopeng. Untuk informasi selengkapnya, lihat Menggunakan inst SageMaker ans notebook Amazon di Panduan SageMaker Pengembang Amazon.
- Putar kredenSIAL yang terbuka — Jika buku catatan berisi kredenSIAL, perlakukan kredenSIAL tersebut sebagai disusupi. Nonaktifkan dan putar kredenSIAL, lalu tinjau log audit dari sistem yang terpengaruh untuk penggunaan nilai-nilai yang diekspos. Ambil rahasia pada waktu berjalan dari AWS Secrets Manager melalui peran eksekusi yang bercakupan sempit alih-alih menyematkannya dalam konten buku catatan. Untuk informasi selengkapnya, lihat Mem AWS Secrets Manager utar rahasia di Panduan AWS Secrets Manager Pengguna.
- Batasi siapa yang dapat membuka instance buku catatan — Berikan akses hanya ke identitas IAM yang membutuhkannya. Lingkup peran eksekusi ke tindakan dan sumber daya tertentu yang digunakan notebook. Kontrol siapa yang dapat membuka buku catatan dengan membatasi `sagemaker:CreatePresignedNotebookInstanceUrl` izin. Untuk informasi selengkapnya, lihat contoh kebijakan SageMaker berbasis identitas Amazon di Panduan Peng SageMaker embang Amazon.

- Enkripsi penyimpanan notebook saat diam — Lampirkan AWS KMS kunci ke instance notebook sehingga volume penyimpanan yang menyimpan file notebook dan pos pemeriksaan dienkripsi saat diam. Gunakan kunci yang dikelola pelanggan sehingga Anda mengontrol kebijakan kunci. Ber `kms:Decrypt` ikan kunci itu hanya untuk identitas yang perlu membaca buku catatan. Untuk informasi selengkapnya, lihat Melindungi data saat diam menggunakan enkripsi di Panduan SageMaker Pengembang Amazon.
- Memantau akses ke instance notebook — T AWS CloudTrail injau `sagemaker:CreatePresignedNotebookInstanceUrl` panggilan dan akses dari identitas atau sumber yang tidak terduga. Untuk informasi selengkapnya, lihat Log panggilan Amazon SageMaker API dengan AWS CloudTrail di Panduan SageMaker Pengembang Amazon.

Ciri-ciri dampak untuk inst SageMaker ans notebook Amazon

Sifat dampak menggambarkan radius ledakan potensial dari suatu eksposur. Security Hub menganalisis izin efektif dari prinsipal yang AWS Identity and Access Management terkait dengan instance SageMaker notebook untuk menentukan sumber daya hilir yang dapat dijangkau penyerang jika instance notebook dikompromikan. Setiap sifat dampak mengidentifikasi pola eskalasi hak istimewa tertentu. Untuk mengurangi radius ledakan Anda, tinjau jalur izin yang dijelaskan di setiap sifat dan hapus hak istimewa yang tidak perlu.

Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa paling sedikit dengan hanya memberikan izin yang diperlukan untuk melakukan tugas. Ganti kebijakan luas dengan kebijakan cakupan yang hanya memberikan tindakan dan sumber daya spesifik yang dibutuhkan. Untuk mengidentifikasi izin yang tidak digunakan untuk dihapus, gunakan Penganalisis Akses IAM untuk menghasilkan rekomendasi berdasarkan riwayat akses. Untuk informasi selengkapnya, lihat Temuan untuk akses eksternal dan tidak digunakan dan M enerapkan izin hak istimewa terkecil di Panduan Pengguna IAM.

Memiliki jalur eksekutor istimewa kontrol penuh

Prinsipal terkait dapat meneruskan peran ke dan menyuntikkan kode ke sumber daya komputasi yang sudah memiliki izin tinggi. Hal ini memungkinkan prinsipal untuk mendapatkan kontrol penuh atas pelaksana dan melakukan tindakan apa pun yang diizinkan oleh peran pelaksana.

Memiliki jalur eskalasi kebijakan langsung

Prinsipal terkait dapat secara langsung memodifikasi kebijakan IAM untuk memberikan izin tambahan kepada dirinya sendiri, meningkatkan hak istimewanya sendiri tanpa sumber daya perantara.

Memiliki jalur pembajakan kebijakan kepercayaan

Prinsipal terkait dapat memodifikasi kebijakan kepercayaan dari peran IAM untuk membiarkan dirinya mengambil peran itu, mendapatkan izin peran tersebut.

Memiliki jalur data ransomware

Prinsipal terkait dapat mengenkripsi atau menghapus data dengan cara yang dapat digunakan untuk ransomware, seperti mengenkripsi objek Amazon S3 dengan kunci yang dikelola pelanggan dan kemudian memodifikasi kebijakan AWS KMS kunci.

Telah menghapus jalur pembatasan

Prinsipal terkait dapat menghapus batasan keamanan seperti batas izin, kebijakan kontrol layanan, atau pernyataan penolakan kebijakan berbasis sumber daya, memperluas apa yang dapat dilakukan oleh prinsipal lain atau sumber daya itu sendiri.

Memiliki jalur pass role buat eksekutor

Prinsipal terkait dapat membuat sumber daya komputasi baru (seperti fungsi Lambda atau instans Amazon EC2) dan memberikannya peran istimewa, secara efektif mencuci izinnya sendiri melalui sumber daya baru.

Memiliki jalur pelaksana peran swap yang ada

Prinsip terkait dapat mengubah peran IAM yang dilampirkan ke sumber daya komputasi yang ada, menggantinya dengan peran yang lebih istimewa untuk meningkatkan akses.

Memiliki jalur eskalasi rantai peran

Prinsipal terkait dapat mengambil urutan peran, di mana setiap peran dalam rantai memiliki izin yang semakin luas, pada akhirnya mencapai peran yang sangat istimewa.

Telah menyuntikkan jalur eksekutor istimewa kode

Prinsip terkait dapat menyuntikkan kode ke sumber daya komputasi yang sedang berjalan yang memiliki izin tinggi, menjalankan operasi arbitrer di bawah peran istimewa sumber daya tersebut.

Telah menonaktifkan jalur jejak audit

Prinsipal terkait dapat menonaktifkan layanan logging atau pemantauan seperti CloudTrail, secara efektif menutupi jejaknya selama atau setelah eskalasi.

Memiliki akses jalur eksekutor yang ada

Prinsipal terkait dapat memanggil atau menghubungkan ke sumber daya komputasi yang ada dan menggunakan peran terlampir untuk melakukan tindakan istimewa.

Memiliki jalur pencetakan kredensi

Prinsipal terkait dapat membuat kredenSIAL jangka panjang baru (seperti kunci akses atau profil login) untuk prinsipal lain, membuat jalur akses persisten yang bertahan dari rotasi kata sandi atau kedaluwarsa sesi.

Memiliki jalur akses data peran pass

Prinsipal terkait dapat membuat sumber daya layanan dan memberikannya peran yang memiliki akses ke data sensitif, mendapatkan akses tidak langsung ke data tersebut melalui sumber daya baru.

Memiliki jalur pembajakan tugas peran lulus

Prinsip terkait dapat meneruskan peran ke tugas yang dijadwalkan atau didorong oleh peristiwa (seperti fungsi Lambda yang dipicu oleh suatu peristiwa), memungkinkannya untuk mengeksekusi kode arbitrer dengan izin peran tersebut.

Memiliki jalur akses data hop tunggal

Prinsipal terkait dapat langsung mengakses sumber daya data sensitif (seperti bucket Amazon S3 atau tabel DynamoDB) melalui izin yang ada, tanpa memerlukan langkah eskalasi menengah.

Memiliki jalur kemajuan kemampuan

Prinsipal terkait memiliki jalur eskalasi hak istimewa yang memajukan kemampuan keseluruhannya melampaui apa yang disarankan oleh izin yang ditetapkan secara langsung. Ini adalah klasifikasi umum untuk jalur yang tidak cocok dengan pola yang lebih spesifik.

Memperbaiki eksposur untuk mesin virtual Azure

AWS Security Hub dapat menghasilkan temuan eksposur untuk mesin virtual Azure.

Pada konsol Hub Keamanan, mesin virtual Azure yang terlibat dalam penemuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat kesalahan konfigurasi untuk mesin virtual Azure
  - Mesin virtual Azure memiliki grup keamanan jaringan terbuka
  - Mesin virtual Azure memiliki aturan keamanan yang memungkinkan akses SSH atau RDP
  - Peran yang terkait dengan mesin virtual Azure memiliki penetapan peran akses administratif
  - Mesin virtual Azure memiliki sistem operasi akhir masa pakai
- Sifat jangkauan untuk mesin virtual Azure
  - Mesin virtual Azure dapat dijangkau melalui internet
- Ciri-ciri kerentanan untuk mesin virtual Azure
  - Mesin virtual Azure memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi
  - Mesin virtual Azure memiliki kerentanan perangkat lunak
  - Mesin virtual Azure memiliki paket perangkat lunak berbahaya

Sifat kesalahan konfigurasi untuk mesin virtual Azure

Berikut adalah sifat kesalahan konfigurasi untuk mesin virtual Azure dan langkah-langkah remediasi yang disarankan.

Mesin virtual Azure memiliki grup keamanan jaringan terbuka

Grup keamanan jaringan (NSG) bertindak sebagai firewall virtual untuk mesin virtual Azure Anda, memfilter lalu lintas masuk dan keluar dengan seperangkat aturan keamanan yang diprioritaskan. Grup keamanan jaringan terbuka berisi aturan yang memungkinkan akses tidak terbatas dari sumber apa pun (misalnya, sumber `Any` atau`0.0.0.0/0`). Aturan-aturan ini dapat mengekspos mesin virtual Anda ke akses tidak sah dari internet. Mengikuti prinsip-prinsip keamanan standar, batasi aturan grup keamanan jaringan hanya untuk alamat IP, port, dan protokol tertentu yang diperlukan beban kerja Anda.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau aturan grup keamanan jaringan dan menilai konfigurasi saat ini

Identifikasi grup keamanan jaringan yang terkait dengan antarmuka jaringan atau subnet mesin virtual, dan tinjau aturan keamanan masuknya. Evaluasi port mana yang memungkinkan lalu lintas dari rentang sumber yang luas, seperti `Any` atau`0.0.0.0/0`. Aturan diproses dalam urutan prioritas, jadi konfirmasikan bahwa aturan permisif tidak diutamakan daripada aturan yang lebih ketat. Untuk informasi selengkapnya, lihat Grup keamanan jaringan dalam dokumentasi Microsoft Azure.

Batasi aturan grup keamanan jaringan

Ubah atau hapus aturan yang memungkinkan akses tidak terbatas. Ganti sumber yang luas seperti `Any` dengan alamat IP tepercaya tertentu, rentang CIDR, tag layanan, atau grup keamanan aplikasi yang memerlukan akses. Batasi rentang port tujuan hanya pada port yang digunakan beban kerja Anda. Untuk informasi selengkapnya, lihat Mengelola grup keamanan jaringan di dokumentasi Microsoft Azure.

Mesin virtual Azure memiliki aturan keamanan yang memungkinkan akses SSH atau RDP

Protokol manajemen jarak jauh seperti SSH (port 22) dan RDP (port 3389) memungkinkan pengguna terhubung ke dan mengelola mesin virtual Azure dari lokasi jarak jauh. Ketika aturan grup keamanan jaringan mengizinkan port-port ini dari internet (sumber `Any` atau`0.0.0.0/0`), permukaan serangan mesin virtual Anda meningkat secara signifikan dan menjadi terkena serangan brute-force dan berbasis kredensi. Mengikuti prinsip-prinsip keamanan standar, batasi akses jarak jauh ke alamat IP tertentu dan tepercaya, atau hapus akses internet langsung ke port ini sepenuhnya.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Batasi aturan grup keamanan jaringan

Batasi akses SSH dan RDP ke alamat IP tepercaya tertentu atau rentang CIDR sebagai `Any` gantinya, atau hapus aturan masuk jika akses jarak jauh dari internet tidak diperlukan. Untuk informasi selengkapnya, lihat Mengelola grup keamanan jaringan di dokumentasi Microsoft Azure.

Gunakan Azure Bastion untuk konektivitas yang aman

Alih-alih mengekspos port SSH atau RDP ke internet, gunakan Azure Bastion untuk terhubung ke mesin virtual Anda melalui TLS tanpa alamat IP publik atau membuka port masuk. Untuk informasi selengkapnya, lihat Azure Bastion di dokumentasi Microsoft Azure.

Gunakan akses mesin virtual tepat waktu

Aktifkan akses mesin virtual just-in-time (JIT) di Microsoft Defender for Cloud sehingga port manajemen seperti SSH dan RDP tetap tertutup secara default dan terbuka hanya untuk permintaan terikat waktu yang disetujui dari alamat IP sumber tertentu. Untuk informasi selengkapnya, lihat Mengaktifkan akses tepat waktu di dokumentasi Microsoft Azure.

Peran yang terkait dengan mesin virtual Azure memiliki penetapan peran akses administratif

Anda dapat menetapkan identitas terkelola ke mesin virtual Azure dan memberikannya penetapan peran kontrol akses berbasis peran Azure (Azure RBAC) untuk mengakses sumber daya Azure lainnya. Ketika identitas terkait memiliki penetapan peran administratif (seperti `Owner` atau`Contributor`) pada lingkup yang luas, biasanya memberikan izin jauh melampaui apa yang dibutuhkan beban kerja. Jika mesin virtual dikompromikan, penyerang dapat menggunakan izin berlebihan ini untuk bergerak secara lateral melintasi lingkungan Anda, mengakses data, atau memanipulasi sumber daya. Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa paling sedikit dengan menetapkan hanya izin yang dibutuhkan beban kerja.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Meninjau dan mengidentifikasi penugasan peran administratif

Di portal Azure, tinjau penugasan peran untuk identitas yang terkait dengan mesin virtual. Cari peran administrator istimewa seperti`Owner`,, atau `Contributor`User Access Administrator, dan untuk peran khusus yang menggunakan wildcard (`*`) di dalamnya. `Actions` Untuk informasi selengkapnya, lihat Daftar penetapan peran Azure di dokumentasi Microsoft Azure.

Terapkan akses hak akses paling rendah

Ganti penetapan peran administratif dengan peran bawaan yang paling tidak memiliki hak istimewa yang hanya memberikan izin yang dibutuhkan beban kerja. Tetapkan pada lingkup tersempit (sumber daya atau grup sumber daya) yang memenuhi kebutuhan Anda. Saat membuat peran khusus, tentukan `Actions` dan `DataActions` secara eksplisit alih-alih menggunakan wildcard. Untuk informasi selengkapnya, lihat Praktik terbaik untuk Azure RBAC di dokumentasi Microsoft Azure.

Mesin virtual Azure memiliki sistem operasi akhir masa pakai

Mesin virtual Azure menjalankan sistem operasi akhir masa pakai yang tidak lagi didukung atau dikelola oleh vendornya. Ketika sistem operasi mencapai akhir masa pakai, vendor berhenti merilis pembaruan keamanan dan saran, yang membuat kerentanan yang diketahui secara permanen tidak ditambal dan membuat mesin virtual diserang. Mengikuti praktik terbaik keamanan, tingkatkan ke versi sistem operasi yang didukung.

Remediasi: Tingkatkan ke versi sistem operasi yang didukung

Rencanakan peningkatan di tempat atau migrasikan beban kerja ke mesin virtual yang menjalankan versi sistem operasi yang didukung. Sebelum memutakhirkan, konfirmasikan kompatibilitas aplikasi dan ambil cadangan atau snapshot sehingga Anda dapat memutar kembali jika diperlukan. Untuk Windows, ikuti panduan peningkatan di tempat; untuk Linux, ikuti panduan peningkatan dari vendor distribusi Anda. Untuk informasi selengkapnya, lihat Melakukan peningkatan VM Windows Server di tempat di dokumentasi Microsoft Azure.

Sifat jangkauan untuk mesin virtual Azure

Berikut adalah ciri-ciri jangkauan untuk mesin virtual Azure dan langkah-langkah remediasi yang disarankan.

Mesin virtual Azure dapat dijangkau melalui internet

Mesin virtual Azure dengan port yang dapat dijangkau dari internet mungkin terkena serangan. Mesin virtual dapat dijangkau ketika memiliki alamat IP publik. Ini juga dapat dijangkau ketika penyeimbang beban, gateway aplikasi, atau jalur jaringan lainnya mengizinkan lalu lintas masuk dari internet. Mengikuti prinsip-prinsip keamanan standar, terapkan kontrol akses jaringan dengan hak istimewa terendah dengan membatasi lalu lintas masuk hanya ke sumber dan port yang diperlukan.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Batasi atau hapus eksposur internet

Tinjau apakah mesin virtual memerlukan alamat IP publik. Jika tidak, pisahkan alamat IP publik dari antarmuka jaringan dan gunakan alamat IP pribadi sebagai gantinya. Jika konektivitas internet keluar masih diperlukan, gunakan gateway NAT.

Jika akses masuk diperlukan, letakkan mesin virtual di belakang penyeimbang beban, Azure Firewall, atau gateway aplikasi daripada mengeksposnya secara langsung. Untuk informasi selengkapnya, lihat Alamat IP Pu blik di dokumentasi Microsoft Azure.

Kencangkan aturan grup keamanan jaringan masuk

Ubah atau hapus aturan grup keamanan jaringan masuk yang mengizinkan akses tidak terbatas (Anyatau`0.0.0.0/0`), dan batasi akses ke rentang sumber tertentu, port, dan protokol yang dibutuhkan beban kerja Anda. Untuk informasi selengkapnya, lihat Grup keamanan jaringan dalam dokumentasi Microsoft Azure.

Gunakan Azure Bastion untuk akses manajemen

Untuk konektivitas manajemen, gunakan Azure Bastion untuk menjangkau mesin virtual melalui TLS tanpa alamat IP publik atau port terbuka SSH/RDP . Untuk informasi selengkapnya, lihat Azure Bastion di dokumentasi Microsoft Azure.

Ciri-ciri kerentanan untuk mesin virtual Azure

Berikut adalah ciri-ciri kerentanan untuk mesin virtual Azure dan langkah-langkah remediasi yang disarankan.

Mesin virtual Azure memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

Kerentanan dan Eksposur Umum (CVE) dapat memengaruhi paket perangkat lunak yang diinstal pada mesin virtual Azure. Kerentanan prioritas tinggi dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi. Ini merupakan ancaman keamanan langsung karena kode eksploitasi mungkin sudah tersedia untuk umum dan secara aktif digunakan oleh penyerang atau alat pemindaian otomatis. Menambal kerentanan ini segera untuk melindungi mesin virtual Anda.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau dan memperbaiki temuan

Gunakan penilaian kerentanan Microsoft Defender for Cloud untuk meninjau CVE yang terkena dampak dan langkah-langkah perbaikan untuk mesin virtual. Panel detail untuk setiap temuan mencakup CV yang relevan dan remediasi yang direkomendasikan. Untuk informasi selengkapnya, lihat Memperbaiki kerentanan mesin dalam dokumentasi Microsoft Azure.

Terapkan pembaruan

Gunakan Azure Update Manager untuk menilai dan menyebarkan pembaruan sistem operasi dan perangkat lunak di seluruh mesin virtual Anda sesuai jadwal. Jika pembaruan tidak tersedia, pertimbangkan untuk menghapus atau menonaktifkan perangkat lunak yang rentan, atau membatasi akses jaringan ke sana, sampai patch dirilis. Untuk informasi selengkapnya, lihat Azure Update Manager di dokumentasi Microsoft Azure.

Pertimbangan masa depan

Untuk mencegah kejadian di masa mendatang, aktifkan Microsoft Defender for Server untuk terus memindai mesin virtual Anda untuk kerentanan, dan buat jadwal tambalan reguler dengan Azure Update Manager. Untuk informasi selengkapnya, lihat Microsoft Defender untuk Server di dokumentasi Microsoft Azure.

Mesin virtual Azure memiliki kerentanan perangkat lunak

Kerentanan dan Eksposur Umum (CVE) dapat memengaruhi paket perangkat lunak yang diinstal pada mesin virtual Azure. Kerentanan nonkritis mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitabilitas yang lebih rendah daripada kerentanan prioritas tinggi. Meskipun mereka menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Mengikuti praktik terbaik keamanan, tambal kerentanan ini untuk melindungi mesin virtual Anda dari serangan.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Tinjau dan memperbaiki temuan

Gunakan penilaian kerentanan Microsoft Defender for Cloud untuk meninjau CVE yang terkena dampak dan ikuti langkah-langkah perbaikan di panel rincian pencarian. Untuk informasi selengkapnya, lihat Memperbaiki kerentanan mesin dalam dokumentasi Microsoft Azure.

Terapkan pembaruan

Gunakan Azure Update Manager untuk menilai dan menyebarkan pembaruan sistem operasi dan perangkat lunak di seluruh mesin virtual Anda. Untuk mengelola pembaruan secara konsisten dalam skala besar, konfigurasikan tambalan terjadwal. Untuk informasi selengkapnya, lihat Azure Update Manager di dokumentasi Microsoft Azure.

Mesin virtual Azure memiliki paket perangkat lunak berbahaya

Paket berbahaya adalah komponen perangkat lunak yang berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. Paket berbahaya menimbulkan ancaman aktif dan kritis terhadap mesin virtual Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan terpisah. Mengikuti praktik terbaik keamanan, hapus paket berbahaya untuk melindungi mesin virtual Anda dari potensi serangan.

Remediasi: Selidiki dan hapus paket berbahaya

Tinjau detail temuan untuk memahami ancaman dan mengidentifikasi paket yang terkena dampak, lalu hapus paket yang diidentifikasi menggunakan manajer paket yang sesuai untuk sistem operasi. Setelah penghapusan, jalankan pemindaian untuk mengonfirmasi bahwa tidak ada komponen berbahaya terkait yang tersisa. Untuk informasi selengkapnya, lihat Microsoft Defender untuk Server di dokumentasi Microsoft Azure.

Memperbaiki eksposur untuk wadah blob Azure Storage

AWS Security Hub dapat menghasilkan temuan eksposur untuk wadah blob Azure Storage.

Pada konsol Hub Keamanan, wadah blob Azure Storage yang terlibat dalam penemuan eksposur dan informasi pengenalnya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan

menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat jangkauan untuk wadah blob Azure Storage
  - Akun penyimpanan memungkinkan akses blob anonim
- Sifat kesalahan konfigurasi untuk wadah blob Azure Storage
  - Akun penyimpanan tidak memerlukan HTTPS untuk operasi transfer
  - Akun penyimpanan tidak dienkripsi dengan kunci yang dikelola pelanggan
  - Akun penyimpanan memungkinkan akses lintas penyewa
  - Akun penyimpanan menonaktifkan penghapusan lunak blob
  - Akun penyimpanan memungkinkan penghapusan permanen gumpalan yang dihapus dengan lunak
  - Wadah blob Azure Storage menonaktifkan versi blob
  - Wadah penyimpanan tidak memiliki kebijakan kekekalan

Sifat jangkauan untuk wadah blob Azure Storage

Berikut adalah ciri-ciri jangkauan untuk wadah blob Azure Storage dan langkah-langkah remediasi yang disarankan.

Akun penyimpanan memungkinkan akses blob anonim

Ketika akses baca anonim diaktifkan, klien yang tidak diautentikasi dapat membaca data blob tanpa otorisasi. Ketika akun penyimpanan mengizinkan akses blob anonim (publik) dan tingkat akses wadah mengizinkannya, siapa pun di internet publik dapat membaca data dalam wadah itu. Mengikuti prinsip-prinsip keamanan standar, larang akses anonim di tingkat akun dan minta setiap permintaan untuk diotorisasi, kecuali skenario Anda secara eksplisit bergantung pada akses baca publik.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Melarang akses anonim untuk akun penyimpanan

Setel `AllowBlobPublicAccess` properti akun penyimpanan ke`false`. Melarang akses anonim di tingkat akun mengesampingkan pengaturan akses semua kontainer di akun dan memblokir permintaan anonim di masa mendatang. Untuk informasi selengkapnya, lihat Mencegah akses baca anonim di dokumentasi Microsoft Azure.

Atur tingkat akses kontainer ke pribadi

Jika kontainer individual dikonfigurasi untuk akses publik, setel tingkat akses anonim setiap kontainer `Private` sehingga semua permintaan memerlukan otorisasi. Sebelum mengubah pengaturan, tinjau aplikasi klien yang mungkin bergantung pada akses anonim. Untuk informasi selengkapnya, lihat Meng konfigurasi akses baca anonim di dokumentasi Microsoft Azure.

Sifat kesalahan konfigurasi untuk wadah blob Azure Storage

Berikut adalah sifat kesalahan konfigurasi untuk wadah blob Azure Storage dan langkah-langkah remediasi yang disarankan.

Akun penyimpanan tidak memerlukan HTTPS untuk operasi transfer

Ketika akun penyimpanan tidak memerlukan transfer aman, ia menerima permintaan melalui HTTP yang tidak terenkripsi. Data dan kredenSIAL yang dikirim melalui HTTP dapat dicegat atau dimodifikasi dalam transit oleh penyerang di jalur jaringan. Mengikuti prinsip keamanan standar, memerlukan transfer aman sehingga akun menerima permintaan hanya melalui HTTPS.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Memerlukan transfer yang aman

Aktif kan properti yang diperlukan transfer aman pada akun penyimpanan (`enableHttpsTrafficOnly`properti). Ketika transfer aman diperlukan, permintaan apa pun yang dibuat melalui HTTP ditolak. Untuk informasi selengkapnya, lihat Memerlukan transfer aman di dokumentasi Microsoft Azure.

Menerapkan versi TLS minimum

Setel versi TLS minimum akun penyimpanan ke 1.2 (`minimumTlsVersion`properti) sehingga permintaan yang menggunakan versi protokol yang lebih lama dan kurang aman ditolak. Konfirmasikan bahwa klien Anda mendukung TLS 1.2 sebelum Anda menerapkan pengaturan ini. Untuk informasi selengkapnya, lihat Meng onfigurasi versi TLS minimum untuk akun penyimpanan di dokumentasi Microsoft Azure.

Akun penyimpanan tidak dienkripsi dengan kunci yang dikelola pelanggan

Secara default, Azure Storage mengenkripsi data saat diam dengan Microsoft-managed kunci. Customer-managed kunci (CMK) memberi Anda kontrol atas kunci yang melindungi data Anda, termasuk kemampuan untuk memutar, mencabut, dan mengaudit akses ke kunci. Jika persyaratan kepatuhan organisasi Anda memerlukan kontrol atas kunci enkripsi, tidak adanya kunci yang dikelola pelanggan adalah celah. Mengikuti praktik terbaik perlindungan data, konfigurasikan akun penyimpanan untuk menggunakan kunci yang dikelola pelanggan yang disimpan di Azure Key Vault atau HSM terkelola.

Remediasi: Konfigurasikan kunci yang dikelola pelanggan

Simpan kunci di Azure Key Vault atau Azure Key Vault Managed HSM, dengan perlindungan penghapusan dan pembersihan lunak diaktifkan. Berikan identitas terkelola `getwrapkey`,, dan `unwrapkey` izin, lalu konfigurasikan akun penyimpanan untuk menggunakan kunci tersebut untuk enkripsi. Anda dapat beralih antara yang dikelola pelanggan dan Microsoft-managed kunci kapan saja. Untuk informasi selengkapnya, lihat Customer-managed kunci untuk enkripsi penyimpanan dalam dokumentasi Microsoft Azure.

Akun penyimpanan memungkinkan akses lintas penyewa

Cross-tenant pengaturan akses, seperti replikasi objek lintas penyewa atau delegasi tanda tangan akses bersama lintas penyewa (SAS), dapat menyebabkan data meninggalkan penyewa Microsoft Entra yang memiliki akun penyimpanan. Jika beban kerja Anda tidak memerlukan berbagi data di seluruh penyewa, membiarkan pengaturan ini diaktifkan meningkatkan risiko data meninggalkan batas penyewa Anda. Mengikuti prinsip keamanan standar, nonaktifkan akses lintas penyewa kecuali diperlukan secara eksplisit.

Remediasi: Nonaktifkan pengaturan akses lintas penyewa

Pada akun penyimpanan, nonaktifkan replikasi objek lintas penyewa (disetel `allowCrossTenantReplication` kefalse) dan, jika didukung, batasi delegasi SAS lintas-penyewa. Tinjau persyaratan replikasi dan berbagi sebelum melakukan perubahan. Untuk informasi selengkapnya, lihat ikhtisar akun Azure Storage di dokumentasi Microsoft Azure.

Akun penyimpanan menonaktifkan penghapusan lunak blob

Blob soft delete melindungi gumpalan, snapshot, dan versi individual dari penghapusan dan penggantian yang tidak disengaja atau berbahaya. Ini menyimpan data yang dihapus untuk periode retensi yang dapat dikonfigurasi, di mana Anda dapat memulihkannya. Ketika penghapusan lunak dinonaktifkan, data blob yang dihapus atau diganti tidak dapat dipulihkan, yang menyebabkan akun Anda kehilangan data permanen. Mengikuti praktik terbaik perlindungan data, aktifkan penghapusan lunak blob dengan periode retensi yang sesuai.

Remediasi: Aktifkan penghapusan lembut blob

Aktifkan penghapusan lunak blob pada akun penyimpanan dan tetapkan periode retensi (1 hingga 365 hari) yang memenuhi persyaratan pemulihan Anda. Untuk perlindungan yang lebih lengkap, aktifkan penghapusan lunak wadah dan versi blob juga. Untuk informasi selengkapnya, lihat Penghapusan lunak untuk blob di dokumentasi Microsoft Azure.

Akun penyimpanan memungkinkan penghapusan permanen gumpalan yang dihapus dengan lunak

Ketika penghapusan permanen diizinkan (`allowPermanentDelete`propertinya`true`), gumpalan dan snapshot yang dihapus dengan lembut dapat dihapus sebelum periode retensi penghapusan lunak berakhir. Ini merusak perlindungan yang disediakan oleh soft delete, karena pengguna atau prinsipal yang dikompromikan dapat secara permanen menghancurkan data yang dapat dipulihkan sebelum periode penyimpanan berakhir. Mengikuti praktik terbaik perlindungan data, jangan izinkan penghapusan permanen gumpalan yang dihapus lunak kecuali Anda memiliki persyaratan khusus yang dipahami dengan baik.

Remediasi: Nonaktifkan penghapusan permanen

Setel `allowPermanentDelete` properti akun penyimpanan agar gumpal `false` an dan snapshot yang dihapus secara lunak tetap dapat dipulihkan selama periode penyimpanan penuh. Untuk informasi selengkapnya, lihat Penghapusan lunak untuk blob di dokumentasi Microsoft Azure.

Wadah blob Azure Storage menonaktifkan versi blob

Pembuatan versi blob secara otomatis mempertahankan versi blob sebelumnya. Ketika gumpalan dimodifikasi atau dihapus, status sebelumnya dipertahankan sebagai versi sebelumnya yang dapat Anda pulihkan. Saat pembuatan versi dinonaktifkan, penulisan ulang dan penghapusan tidak dapat dikembalikan ke status sebelumnya, yang meningkatkan risiko kehilangan atau kerusakan data yang tidak dapat dipulihkan. Mengikuti praktik terbaik perlindungan data, aktifkan versi blob, bersama dengan penghapusan lunak, untuk perlindungan data yang optimal.

Remediasi: Aktifkan pembuatan versi blob

Aktifkan pembuatan versi pada layanan blob akun penyimpanan. Untuk mengontrol biaya mempertahankan banyak versi, gunakan kebijakan manajemen siklus hidup untuk menghapus versi lama secara otomatis. Untuk informasi selengkapnya, lihat Pembuatan versi Blob di dokumentasi Microsoft Azure.

Wadah penyimpanan tidak memiliki kebijakan kekekalan

Kebijakan kekekalan menyimpan data blob dalam status WORM (Write Once, Read Many). Dalam keadaan ini, data tidak dapat dimodifikasi atau dihapus untuk interval tertentu (kebijakan penyimpanan berbasis waktu) atau sampai penahanan legal dihapus. Tanpa kebijakan kekekalan, data penting bisnis atau yang relevan dengan kepatuhan dalam wadah dapat diganti atau dihapus, termasuk oleh pengguna yang memiliki hak istimewa. Jika persyaratan peraturan atau integritas data berlaku, konfigurasikan kebijakan kekekalan untuk wadah.

Remediasi: Konfigurasikan kebijakan kekekalan

Konfigurasikan kebijakan retensi berbasis waktu atau penahanan legal pada wadah. Mengunci kebijakan berbasis waktu saat pengujian selesai sehingga data terlindungi sepenuhnya dalam status WORM. Aktifkan penghapusan lunak sebelum menerapkan kebijakan kekekalan untuk perlindungan tambahan. Untuk informasi selengkapnya, lihat Penyimpanan yang tidak dapat diubah untuk data blob di dokumentasi Microsoft Azure.

Memperbaiki eksposur untuk database Azure SQL

AWS Security Hub dapat menghasilkan temuan eksposur untuk database Azure SQL.

Pada konsol Security Hub, database Azure SQL yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan

menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat kesalahan konfigurasi untuk database Azure SQL
  - Basis data Azure SQL mengaktifkan akses jaringan publik
  - Database Azure SQL tidak menerapkan AD-only otentikasi Azure
  - Database Azure SQL menggunakan nama pengguna admin default atau umum
  - Basis data Azure SQL memiliki cadangan geo-redundan dinonaktifkan

Sifat kesalahan konfigurasi untuk database Azure SQL

Berikut adalah sifat kesalahan konfigurasi untuk database Azure SQL dan langkah-langkah remediasi yang disarankan.

Basis data Azure SQL mengaktifkan akses jaringan publik

Ketika akses jaringan publik diaktifkan pada server logis, database dapat dijangkau melalui titik akhir publik dan dapat menerima koneksi dari internet publik (tunduk pada aturan firewall). Titik akhir publik meningkatkan permukaan serangan database Anda dan mengeksposnya ke upaya koneksi yang tidak sah. Mengikuti prinsip-prinsip keamanan standar, nonaktifkan akses jaringan publik dan sambungkan ke database secara pribadi, atau batasi ketat aturan firewall server.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Nonaktifkan akses jaringan publik dan gunakan Private Link

Atur akses jaringan publik server logis ke `Disabled` dan sambungkan ke database melalui titik akhir pribadi (Azure Private Link) dalam jaringan virtual Anda. Ini menjaga lalu lintas database di tulang punggung Azure dan di luar internet publik. Untuk informasi selengkapnya, lihat Kontrol akses jaringan untuk Azure SQL Database di dokumentasi Microsoft Azure.

Batasi aturan firewall jika akses publik diperlukan

Jika Anda harus tetap mengaktifkan akses publik, hapus aturan apa pun yang memungkinkan jangkauan internet penuh, dan nonaktifkan lz inkan layanan dan sumber daya Azure untuk mengakses server ini saat tidak diperlukan. Batasi aturan firewall tingkat server ke alamat IP tepercaya tertentu yang dibutuhkan beban kerja Anda. Untuk informasi selengkapnya, lihat Kontrol akses jaringan untuk Azure SQL Database di dokumentasi Microsoft Azure.

Menerapkan versi TLS minimum

Setel versi TLS minimum server logis ke 1.2 sehingga koneksi yang menggunakan versi protokol yang lebih lama dan kurang aman ditolak. Konfirmasikan bahwa klien Anda mendukung TLS 1.2 sebelum Anda menerapkan pengaturan ini. Untuk informasi selengkapnya, lihat Pengaturan konektivitas untuk Azure SQL Database di dokumentasi Microsoft Azure.

Database Azure SQL tidak menerapkan AD-only otentikasi Azure

Ketika Entra-only otentikasi Microsoft (sebelumnya AD-only otentikasi Azure) tidak diterapkan, server logis juga menerima otentikasi SQL, yang bergantung pada kata sandi yang disimpan dan dikelola dalam database. Otentikasi SQL lebih rentan terhadap pencurian kredensia dan serangan brute-force dan tidak mendapat manfaat dari kontrol Microsoft Entra terpusat seperti Acces Bersyarat dan otentikasi multifaktor. Mengikuti prinsip keamanan standar, terapkan Entra-only otentikasi Microsoft sehingga hanya identitas Microsoft Entra yang dapat terhubung.

Remediasi: Menerapkan otentikasi Microsoft Entra-only

Tetapkan admin Microsoft Entra untuk server logis, lalu aktifkan Entra-only otentikasi Microsoft. Ini menonaktifkan otentikasi SQL sehingga hanya identitas Microsoft Entra yang dapat terhubung ke server dan database-nya. Konfirmasikan bahwa aplikasi Anda mendukung otentikasi Microsoft Entra sebelum menerapkan pengaturan ini. Untuk informasi selengkapnya, lihat Oten Entra-only tikasi Microsoft di dokumentasi Microsoft Azure.

Database Azure SQL menggunakan nama pengguna admin default atau umum

Login administrator server logis menggunakan nama pengguna yang terkenal atau umum, seperti`sqladmin`,`admin`, atau`sa`. Nama pengguna administrator umum dapat diprediksi, yang membuat server menjadi target yang lebih mudah untuk serangan brute-force dan credential-filling karena penyerang hanya perlu menebak kata sandi. Mengikuti prinsip-prinsip keamanan standar, hindari nama pengguna administrator default atau umum dan pusatkan akses administratif melalui Microsoft Entra ID.

Remediasi: Gunakan administrator non-default dan otentikasi Microsoft Entra

Hindari nama login administrator yang dapat diprediksi. Jika memungkinkan, terapkan Entra-only otentikasi Microsoft dan kelola akses administratif melalui identitas dan grup Microsoft Entra daripada login administrator SQL. Ikuti praktik terbaik keamanan Azure SQL untuk mengelola login dan akses hak istimewa terendah. Untuk informasi selengkapnya, lihat praktik terbaik keamanan Azure SQL Database dalam dokumentasi Microsoft Azure.

Basis data Azure SQL memiliki cadangan geo-redundan dinonaktifkan

Azure SQL Database menyimpan cadangan otomatis dalam penyimpanan geo-redundan secara default, yang mereplikasi cadangan ke wilayah yang dipasangkan dan memungkinkan pemulihan geografis selama pemadaman regional. Ketika redundansi penyimpanan cadangan disetel ke penyimpanan redundan lokal atau penyimpanan redundan zona sebagai gantinya, geo-restore tidak tersedia. Anda tidak dapat memulihkan database di wilayah lain jika wilayah utama menjadi tidak tersedia. Mengikuti praktik terbaik perlindungan data, gunakan penyimpanan cadangan geo-redundan untuk database yang membutuhkan ketahanan terhadap pemadaman regional.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Konfigurasikan penyimpanan cadangan geo-redundan

Atur redundansi penyimpanan cadangan database ke penyimpanan geo-redundant (GRS) atau penyimpanan geo-zone-redundant (GZRS) sehingga geo-restore tersedia. Perubahan berlaku untuk pencadangan di masa mendatang dan dapat memakan waktu hingga 48 jam untuk berlaku. Untuk informasi selengkapnya, lihat Pencadangan otomatis di Azure SQL Database di dokumentasi Microsoft Azure.

Konfigurasikan retensi jangka panjang

Untuk database dengan persyaratan kepatuhan atau pemulihan jangka panjang, konfigurasikan kebijakan retensi jangka panjang (LTR). LTR menyimpan cadangan penuh hingga 10 tahun, selain retensi jangka pendek default. Untuk informasi selengkapnya, lihat Long-term retensi di Azure SQL Database di dokumentasi Microsoft Azure.

Memperbaiki eksposur untuk akun Azure Cosmos DB

AWS Security Hub dapat menghasilkan temuan eksposur untuk akun Azure Cosmos DB.

Pada konsol Hub Keamanan, akun Azure Cosmos DB yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat kesalahan konfigurasi untuk akun Azure Cosmos DB
  - Akun Azure Cosmos DB mengaktifkan akses jaringan publik
  - Akun Azure Cosmos DB tidak menggunakan cadangan berkelanjutan

Sifat kesalahan konfigurasi untuk akun Azure Cosmos DB

Berikut adalah sifat kesalahan konfigurasi untuk akun Azure Cosmos DB dan langkah-langkah remediasi yang disarankan.

Akun Azure Cosmos DB mengaktifkan akses jaringan publik

Ketika akses jaringan publik diaktifkan, akun Azure Cosmos DB dapat dijangkau melalui titik akhir publik. Itu dapat menerima koneksi dari internet publik, tunduk pada firewall dan aturan jaringan virtual. Titik akhir publik meningkatkan permukaan serangan akun Anda dan mengekspos ke upaya koneksi yang tidak sah dan potensi eksfiltrasi data. Mengikuti prinsip keamanan standar, nonaktifkan

akses jaringan publik dan sambungkan ke akun secara pribadi, atau batasi aturan firewall akun dengan ketat.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Nonaktifkan akses jaringan publik dan gunakan Private Link

Tetapkan `publicNetworkAccess` properti akun ke `Disabled` dan sambungkan melalui titik akhir pribadi (Azure Private Link) dalam jaringan virtual Anda. Ketika dikombinasikan dengan kebijakan grup keamanan jaringan yang ketat, titik akhir pribadi membantu mengurangi risiko eksfiltrasi data. Untuk informasi selengkapnya, lihat Mengonfigurasi Azure Private Link di dokumentasi Microsoft Azure.

Batasi aturan firewall jika akses publik diperlukan

Jika Anda harus tetap mengaktifkan akses publik, konfigurasikan aturan firewall IP dan aturan jaringan virtual untuk mengizinkan hanya sumber tepercaya tertentu yang dibutuhkan beban kerja Anda, alih-alih mengizinkan semua jaringan. Untuk informasi selengkapnya, lihat Mengonfigurasi firewall IP di dokumentasi Microsoft Azure.

Akun Azure Cosmos DB tidak menggunakan cadangan berkelanjutan

Dengan mode pencadangan berkelanjutan, Anda dapat menggunakan pemulihan point-in-time untuk memulihkan dari penulisan atau penghapusan yang tidak disengaja. Anda juga dapat mengembalikan database atau wadah yang dihapus ke stempel waktu apa pun dalam periode retensi. Bila akun menggunakan mode pencadangan berkala alih-alih pencadangan berkelanjutan, Anda tidak dapat melakukan pemulihan point-in-time self-service. Batasan ini meningkatkan waktu pemulihan dan risiko kehilangan data setelah perubahan yang tidak disengaja atau berbahaya. Mengikuti praktik terbaik perlindungan data, aktifkan mode pencadangan berkelanjutan di mana beban kerja Anda mendukungnya.

Remediasi: Aktifkan mode pencadangan berkelanjutan

Konfigurasikan akun untuk menggunakan mode pencadangan berkelanjutan (tingkat 7 hari atau 30 hari) sehingga pemulihan point-in-time tersedia. Tinjau batasan saat ini dan API yang didukung sebelum bermigrasi dari pencadangan berkala ke pencadangan berkelanjutan. Untuk informasi selengkapnya, lihat Pencadangan berkelanjutan dengan pemulihan point-in-time di dokumentasi Microsoft Azure.

Memperbaiki eksposur untuk aplikasi Azure Function

AWS Security Hub dapat menghasilkan temuan eksposur untuk aplikasi Azure Function.

Di konsol Security Hub, aplikasi Azure Function yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat kesalahan konfigurasi untuk aplikasi Azure Function
  - Aplikasi Azure Function digunakan di luar VNet
  - Peran yang terkait dengan aplikasi Azure Function memiliki penetapan peran akses administratif
- Ciri-ciri jangkauan untuk aplikasi Azure Function
  - Aplikasi Azure Function memungkinkan pemanggilan pemicu HTTP anonim
- Ciri-ciri kerentanan untuk aplikasi Azure Function
  - Aplikasi Azure Function memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi
  - Aplikasi Azure Function memiliki kerentanan perangkat lunak
  - Aplikasi Azure Function memiliki paket perangkat lunak berbahaya

Sifat kesalahan konfigurasi untuk aplikasi Azure Function

Berikut adalah sifat kesalahan konfigurasi untuk aplikasi Azure Function dan langkah-langkah remediasi yang disarankan.

Aplikasi Azure Function digunakan di luar VNet

Ketika aplikasi Function tidak terintegrasi dengan jaringan virtual, titik akhir dan lalu lintas keluar melintasi jaringan publik daripada batas jaringan pribadi Anda. Bila aplikasi Function tidak terintegrasi dengan jaringan virtual, Anda tidak dapat menerapkan kontrol tingkat jaringan seperti titik akhir pribadi, grup keamanan jaringan, dan akses keluar terbatas. Kesenjangan ini meningkatkan eksposur aplikasi. Mengikuti prinsip-prinsip keamanan standar, integrasikan aplikasi Function dengan jaringan virtual dan gunakan titik akhir pribadi di mana paket hosting Anda mendukungnya.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Integrasikan aplikasi Function dengan jaringan virtual

Aktifkan integrasi jaringan virtual untuk aplikasi Function. Jika didukung oleh paket hosting Anda (Flex Consumption, Elastic Premium, atau Dedicated), gunakan titik akhir pribadi sehingga aplikasi hanya dapat dijangkau dari dalam jaringan Anda. Untuk informasi selengkapnya, lihat opsi jaringan Azure Func tions di dokumentasi Microsoft Azure.

Batasi akses masuk

Pada paket hosting yang tidak mendukung titik akhir pribadi, gunakan pembatasan akses untuk mengizinkan lalu lintas masuk hanya dari rentang alamat IP tepercaya, dan nonaktifkan akses jaringan publik jika tidak diperlukan. Untuk informasi selengkapnya, lihat Meng atur pembatasan akses di dokumentasi Microsoft Azure.

Peran yang terkait dengan aplikasi Azure Function memiliki penetapan peran akses administratif

Anda dapat menetapkan identitas terkelola ke aplikasi Azure Function dan memberikannya penetapan peran kontrol akses berbasis peran Azure (Azure RBAC) untuk mengakses sumber daya Azure lainnya. Ketika identitas terkait memiliki penetapan peran administratif (seperti `Owner` atau`Contributor`) pada cakupan yang luas, biasanya identitas tersebut memberikan izin yang jauh melampaui apa yang dibutuhkan aplikasi. Jika aplikasi Function dikompromikan, penyerang dapat menggunakan izin berlebihan ini untuk bergerak secara lateral melintasi lingkungan Anda,

mengakses data, atau memanipulasi sumber daya. Mengikuti prinsip keamanan standar, berikan hak istimewa paling sedikit dengan menetapkan hanya izin yang dibutuhkan aplikasi.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Meninjau dan mengidentifikasi penugasan peran administratif

Di portal Azure, tinjau penugasan peran untuk identitas yang terkait dengan aplikasi Function. Cari peran administrator istimewa seperti`Owner`,, atau `Contributor`User Access Administrator, dan untuk peran khusus yang menggunakan wildcard (`*`) di dalamnya. `Actions` Untuk informasi selengkapnya, lihat Daftar penetapan peran Azure di dokumentasi Microsoft Azure.

Terapkan akses hak akses paling rendah

Ganti penetapan peran administratif dengan peran bawaan yang paling tidak memiliki hak istimewa yang hanya memberikan izin yang dibutuhkan aplikasi, dan tetapkan pada lingkup tersempit yang memenuhi kebutuhan Anda. Gunakan identitas terkelola alih-alih rahasia yang disimpan untuk koneksi ke layanan Azure lainnya. Untuk informasi selengkapnya, lihat Praktik terbaik untuk Azure RBAC di dokumentasi Microsoft Azure.

Ciri-ciri jangkauan untuk aplikasi Azure Function

Berikut adalah ciri-ciri jangkauan untuk aplikasi Azure Function dan langkah-langkah remediasi yang disarankan.

Aplikasi Azure Function memungkinkan pemanggilan pemicu HTTP anonim

HTTP-triggered Fungsi yang tingkat otorisasinya diatur `anonymous` dapat dipanggil melalui internet tanpa kunci akses atau otentikasi. Pemicu HTTP anonim mengekspos logika fungsi Anda ke pemanggil yang tidak diautentikasi, yang dapat menyebabkan penyalahgunaan, paparan data, atau penolakan dompet melalui pemanggilan yang tidak terkontrol. Mengikuti prinsip-prinsip keamanan standar, memerlukan otentikasi atau kunci akses untuk HTTP-triggered fungsi kecuali akses anonim diperlukan secara eksplisit.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Memerlukan otorisasi untuk pemicu HTTP

Naikkan tingkat otorisasi pemicu HTTP dari `anonymous` ke `function` atau `admin` sehingga permintaan harus menyertakan kunci akses yang valid, dan memerlukan HTTPS. Untuk perlindungan yang lebih kuat, aktifkan App Service Authentication/Authorization atau lanjutkan aplikasi dengan Azure API Management. Untuk informasi selengkapnya, lihat Mengamankan Fungsi Azure di dokumentasi Microsoft Azure.

Memerlukan otentikasi dengan penyedia identitas terkelola

Karena kunci akses adalah kontrol otorisasi dan bukan otentikasi, aktifkan Otentikasi Layanan Aplikasi (Auth Mudah) dengan Microsoft Entra ID sehingga penelepon harus menunjukkan identitas yang valid. Juga nonaktifkan titik akhir administratif (`/admin`rute) ketika mereka tidak diperlukan. Untuk informasi selengkapnya, lihat Mengamankan Fungsi Azure di dokumentasi Microsoft Azure.

Ciri-ciri kerentanan untuk aplikasi Azure Function

Berikut adalah ciri-ciri kerentanan untuk aplikasi Azure Function dan langkah-langkah perbaikan yang disarankan.

Aplikasi Azure Function memiliki kerentanan perangkat lunak yang dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi

Kerentanan dan Eksposur Umum (CVE) dapat memengaruhi paket perangkat lunak dan dependensi di aplikasi Function Anda. Kerentanan prioritas tinggi dapat dieksploitasi jaringan dengan kemungkinan eksploitasi yang tinggi, yang merupakan ancaman keamanan langsung karena kode eksploitasi mungkin sudah tersedia untuk umum dan digunakan secara aktif oleh penyerang. Tambal kerentanan ini segera untuk melindungi aplikasi Function Anda.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Perbarui dependensi yang terpengaruh

Tinjau CV yang terpengaruh dalam temuan, lalu perbarui paket dan dependensi yang rentan ke versi aman terbaru mereka dan gunakan ulang aplikasi. Pertahankan aplikasi Function pada runtime yang didukung sehingga pembaruan keamanan platform terus berlaku. Untuk informasi selengkapnya, lihat Microsoft Defender for App Service di dokumentasi Microsoft Azure.

Pertimbangan masa depan

Untuk mencegah kejadian di masa mendatang, integrasikan pemindaian ketergantungan dan kerentanan ke dalam pipeline build dan penerapan Anda, dan gunakan Microsoft Defender for

Cloud untuk memantau aplikasi Anda untuk temuan konfigurasi dan kerentanan. Untuk informasi selengkapnya, lihat Microsoft Defender for App Service di dokumentasi Microsoft Azure.

Aplikasi Azure Function memiliki kerentanan perangkat lunak

Kerentanan dan Eksposur Umum (CVE) dapat memengaruhi paket perangkat lunak dan dependensi di aplikasi Function Anda. Kerentanan nonkritis mewakili kelemahan keamanan dengan tingkat keparahan atau eksploitabilitas yang lebih rendah daripada kerentanan prioritas tinggi. Meskipun mereka menimbulkan risiko yang kurang langsung, penyerang masih dapat mengeksploitasi kerentanan yang belum ditambal untuk membahayakan kerahasiaan, integritas, atau ketersediaan data, atau untuk mengakses sistem lain. Mengikuti praktik terbaik keamanan, tambal kerentanan ini untuk melindungi aplikasi Function Anda.

Remediasi: Perbarui dependensi yang terpengaruh

Perbarui paket dan dependensi yang rentan ke versi aman terbaru dan gunakan kembali aplikasi. Jika pembaruan tidak tersedia, pertimbangkan untuk menghapus atau menonaktifkan komponen rentan sampai patch dirilis. Untuk informasi selengkapnya, lihat Microsoft Defender for App Service di dokumentasi Microsoft Azure.

Aplikasi Azure Function memiliki paket perangkat lunak berbahaya

Paket berbahaya adalah komponen perangkat lunak yang berisi kode berbahaya yang dirancang untuk membahayakan kerahasiaan, integritas, dan ketersediaan sistem dan data Anda. Paket berbahaya menimbulkan ancaman aktif dan kritis bagi aplikasi Function Anda, karena penyerang dapat mengeksekusi kode berbahaya secara otomatis tanpa mengeksploitasi kerentanan terpisah. Mengikuti praktik terbaik keamanan, hapus paket berbahaya untuk melindungi aplikasi Function Anda dari serangan potensial.

Remediasi: Selidiki dan hapus paket berbahaya

Tinjau detail temuan untuk mengidentifikasi paket yang terpengaruh, menghapusnya dari dependensi proyek Anda, buat ulang dari sumber tepercaya, dan gunakan ulang aplikasi. Setelah remediasi, audit rantai pasokan ketergantungan Anda untuk memastikan tidak ada komponen berbahaya terkait yang tersisa. Untuk informasi selengkapnya, lihat Microsoft Defender for App Service di dokumentasi Microsoft Azure.

Memperbaiki eksposur untuk aplikasi Azure Container

AWS Security Hub dapat menghasilkan temuan eksposur untuk aplikasi Azure Container.

Di konsol Security Hub, aplikasi Azure Container yang terlibat dalam penemuan eksposur dan informasi pengenalnya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat kesalahan konfigurasi untuk aplikasi Azure Container
  - Aplikasi Azure Container memiliki kredensional cleartext dalam variabel lingkungan
  - Aplikasi Azure Container memiliki grup keamanan jaringan terbuka
  - Aplikasi Azure Container memiliki identitas terkelola yang tidak mengikuti hak istimewa
  - Peran yang terkait dengan aplikasi Azure Container memiliki penetapan peran akses administratif
- Sifat jangkauan untuk aplikasi Azure Container
  - Aplikasi Azure Container dapat dijangkau melalui internet

Sifat kesalahan konfigurasi untuk aplikasi Azure Container

Berikut adalah sifat kesalahan konfigurasi untuk aplikasi Azure Container dan langkah-langkah remediasi yang disarankan.

Aplikasi Azure Container memiliki kredensional cleartext dalam variabel lingkungan

Aplikasi Container meneruskan data rahasia, seperti string koneksi, kunci API, atau kata sandi, ke wadah sebagai variabel lingkungan plaintext. Konfigurasi, log, atau wadah yang dikompromikan dapat mengekspos kredenSIAL cleartext dalam variabel lingkungan, yang memungkinkan penyerang menggunakannya kembali untuk mengakses sistem lain. Mengikuti prinsip-prinsip keamanan standar, simpan nilai-nilai sensitif sebagai rahasia dan rujuk mereka daripada menyematkannya dalam plaintext.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Pindahkan kredenSIAL ke rahasia

Ganti nilai variabel lingkungan plaintext dengan rahasia aplikasi Container, atau rahasia referensi yang disimpan di Azure Key Vault. Perbarui wadah untuk membaca nilai dari referensi rahasia tersebut. Putar kredensi apa pun yang sebelumnya diekspos dalam teks biasa. Untuk informasi selengkapnya, lihat Mengelola rahasia di Azure Container Apps di dokumentasi Microsoft Azure.

Gunakan identitas terkelola jika memungkinkan

Untuk koneksi ke layanan Azure yang mendukungnya, gunakan identitas terkelola aplikasi Container alih-alih menyimpan rahasia sama sekali. Untuk informasi selengkapnya, lihat Identitas terkelola di Aplikasi Kontainer Azure di dokumentasi Microsoft Azure.

Aplikasi Azure Container memiliki grup keamanan jaringan terbuka

Grup keamanan jaringan yang melindungi lingkungan aplikasi Container berisi aturan yang mengizinkan akses tak terbatas dari sumber apa pun (misalnya, sumber `Any` atau`0.0.0.0/0`). Grup keamanan jaringan terbuka mengekspos lingkungan aplikasi Container ke akses tidak sah dari internet. Mengikuti prinsip-prinsip keamanan standar, batasi aturan grup keamanan jaringan hanya untuk alamat IP, port, dan protokol tertentu yang diperlukan beban kerja Anda.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Batasi aturan grup keamanan jaringan

Tinjau grup keamanan jaringan yang terkait dengan subnet lingkungan aplikasi Container, dan ubah atau hapus aturan yang mengizinkan akses tidak terbatas. Ganti sumber yang luas seperti

Any dengan rentang tepercaya spesifik yang dibutuhkan beban kerja Anda. Untuk informasi selengkapnya, lihat Jaringan di Aplikasi Kontainer Azure di dokumentasi Microsoft Azure.

Tetapkan batasan masuk IP

Selain aturan grup keamanan jaringan pada subnet lingkungan, konfigurasikan pembatasan masuk IP pada aplikasi kontainer itu sendiri untuk mengizinkan atau menolak lalu lintas masuk berdasarkan rentang alamat IP. Untuk informasi selengkapnya, lihat Meng atur pembatasan masuk IP di Azure Container Apps di dokumentasi Microsoft Azure.

Aplikasi Azure Container memiliki identitas terkelola yang tidak mengikuti hak istimewa

Aplikasi Container memiliki identitas terkelola yang diberikan lebih banyak akses daripada yang dibutuhkan beban kerja. Identitas terkelola yang terlalu istimewa memperluas radius ledakan jika aplikasi Container dikompromikan, karena penyerang dapat bertindak dengan semua izin identitas. Mengikuti prinsip-prinsip keamanan standar, berikan identitas hanya izin yang dibutuhkan beban kerja, pada lingkup tersempit.

Remediasi: Lingkup identitas terkelola hingga hak istimewa terkecil

Tinjau penugasan peran yang diberikan ke identitas terkelola aplikasi Container dan hapus semua yang tidak diperlukan. Tetapkan peran bawaan yang paling tidak memiliki hak istimewa pada lingkup tersempit (sumber daya atau grup sumber daya) yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat Praktik terbaik untuk Azure RBAC di dokumentasi Microsoft Azure.

Peran yang terkait dengan aplikasi Azure Container memiliki penetapan peran akses administratif

Identitas terkelola yang terkait dengan aplikasi Container memiliki penetapan peran administratif (seperti `Owner` atau`Contributor`) pada lingkup yang luas. Tugas ini biasanya memberikan izin jauh melampaui apa yang dibutuhkan beban kerja. Jika aplikasi Container dikompromikan, penyerang dapat menggunakan izin berlebihan ini untuk bergerak secara lateral melintasi lingkungan Anda, mengakses data, atau memanipulasi sumber daya. Mengikuti prinsip keamanan standar, berikan hak istimewa paling sedikit dengan menetapkan hanya izin yang dibutuhkan aplikasi.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Meninjau dan mengidentifikasi penugasan peran administratif

Di portal Azure, tinjau penugasan peran untuk identitas yang terkait dengan aplikasi Container. Cari peran administrator istimewa seperti`Owner`,, atau `Contributor`User Access Administrator`,`

dan untuk peran khusus yang menggunakan wildcard (*) di dalamnya. `Actions` Untuk informasi selengkapnya, lihat Daftar penetapan peran Azure di dokumentasi Microsoft Azure.

Terapkan akses hak akses paling rendah

Ganti penetapan peran administratif dengan peran bawaan yang paling tidak memiliki hak istimewa yang hanya memberikan izin yang dibutuhkan aplikasi, dan tetapkan pada lingkup tersempit yang memenuhi kebutuhan Anda. Untuk informasi selengkapnya, lihat Praktik terbaik untuk Azure RBAC di dokumentasi Microsoft Azure.

Sifat jangkauan untuk aplikasi Azure Container

Berikut adalah ciri-ciri jangkauan untuk aplikasi Azure Container dan langkah-langkah remediasi yang disarankan.

Aplikasi Azure Container dapat dijangkau melalui internet

Aplikasi Container dapat dijangkau dari internet publik, baik karena input eksternal diaktifkan (dis `ingress.external` etel `ketrue`) atau karena lingkungannya memiliki alamat IP publik. Jangkauan publik meningkatkan permukaan serangan aplikasi Container dan mengeksposnya ke permintaan yang tidak sah. Mengikuti prinsip keamanan standar, nonaktifkan input eksternal jika tidak diperlukan, gunakan lingkungan internal, atau letakkan aplikasi di belakang titik masuk yang terkontrol dan diautentikasi.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Batasi atau hapus masuknya eksternal

Setel masuk ke internal jika aplikasi hanya perlu dijangkau dari dalam jaringan atau lingkungan virtual Anda. Jika akses publik diperlukan, batasi dengan batasan IP masuk. Di depan aplikasi dengan gateway seperti Azure Application Gateway atau Azure Front Door.

Gateway ini menyediakan otentikasi dan firewall aplikasi web. Untuk informasi selengkapnya, lihat Ingress di Azure Container Apps di dokumentasi Microsoft Azure.

Gunakan lingkungan internal

Untuk menghindari penetapan alamat IP publik, gunakan aplikasi Container ke lingkungan internal (terintegrasi jaringan virtual) yang menggunakan alamat IP pribadi, dan ekspos hanya titik akhir yang

harus bersifat publik melalui titik masuk terkontrol. Untuk informasi selengkapnya, lihat Jaringan di Aplikasi Kontainer Azure di dokumentasi Microsoft Azure.

Memerlukan HTTPS dan otentikasi untuk masuk publik

Ketika masuk harus tetap publik, nonaktifkan koneksi tidak aman (dis `allowInsecure` et `false` el ke) sehingga lalu lintas hanya dilayani melalui HTTPS. Aktifkan fitur otentikasi bawaan dengan Microsoft Entra ID sehingga permintaan yang tidak diautentikasi ditolak. Untuk informasi selengkapnya, lihat Otentikasi dan otorisasi di Azure Container Apps di dokumentasi Microsoft Azure.

Memperbaiki eksposur untuk cluster Layanan Azure Kubernetes

AWS Security Hub dapat menghasilkan temuan eksposur untuk cluster Azure Kubernetes Service (AKS).

Pada konsol Hub Keamanan, cluster AKS yang terlibat dalam temuan eksposur dan informasi pengenalnya tercantum di bagian Sumber Daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat kesalahan konfigurasi untuk cluster Layanan Azure Kubernetes

  - Cluster Layanan Azure Kubernetes menjalankan versi Kubernetes yang tidak didukung
  - Cluster Layanan Azure Kubernetes memiliki rahasia Kubernetes yang tidak dienkripsi
- Sifat jangkauan untuk cluster Layanan Azure Kubernetes
  - Cluster Layanan Azure Kubernetes memungkinkan akses publik

Sifat kesalahan konfigurasi untuk cluster Layanan Azure Kubernetes

Berikut adalah sifat kesalahan konfigurasi untuk cluster Layanan Azure Kubernetes dan langkah-langkah remediasi yang disarankan.

Cluster Layanan Azure Kubernetes menjalankan versi Kubernetes yang tidak didukung

Cluster AKS menjalankan versi Kubernetes yang tidak lagi didukung oleh Microsoft. Versi Kubernetes yang tidak didukung berhenti menerima tambalan keamanan dan perbaikan bug, yang membuat kerentanan yang diketahui di bidang kontrol dan komponen node tidak ditangani dan membuat cluster diserang. Mengikuti praktik terbaik keamanan, simpan cluster pada versi Kubernetes yang didukung.

Remediasi: Tingkatkan ke versi Kubernetes yang didukung

Tingkatkan bidang kontrol cluster dan kumpulan node ke versi Kubernetes yang didukung. Karena versi minor tidak dapat dilewati, tingkatkan secara berurutan melalui setiap versi minor dan terapkan patch terbaru. Tinjau perubahan besar untuk setiap versi sebelum memutakhirkan.

Pertimbangkan untuk mengaktifkan peningkatan otomatis agar tetap terkini. Untuk informasi selengkapnya, lihat Versi Kubernetes yang didukung di AKS dalam dokumentasi Microsoft Azure.

Cluster Layanan Azure Kubernetes memiliki rahasia Kubernetes yang tidak dienkripsi

Secara default, cluster menyimpan rahasia Kubernetes di penyimpanan data etcd tanpa enkripsi oleh kunci yang dikendalikan pelanggan. Tanpa enkripsi saat diam menggunakan layanan manajemen kunci, siapa pun yang mendapatkan akses ke data etcd yang mendasarinya dapat membaca nilai rahasia sensitif seperti kredenSIAL dan token. Mengikuti praktik terbaik perlindungan data, aktifkan enkripsi KMS etcd sehingga rahasia Kubernetes dienkripsi saat diam dengan kunci di Azure Key Vault.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Aktifkan enkripsi KMS etcd

Konfigurasikan cluster untuk menggunakan enkripsi etcd Key Management Service (KMS) dengan kunci yang disimpan di Azure Key Vault. Berikan identitas cluster mengenkripsi dan mendekripsi izin pada kunci. Re-encrypt rahasia yang ada setelah Anda mengaktifkan fitur. Aktifkan perlindungan penghapusan lunak dan pembersihan pada brankas kunci sehingga kunci tidak dapat hilang. Untuk informasi selengkapnya, lihat enkripsi KMS etcd di AKS dalam dokumentasi Microsoft Azure.

Aktifkan perlindungan penghapusan lunak dan pembersihan pada brankas kunci sehingga kunci tidak dapat hilang. Untuk informasi selengkapnya, lihat enkripsi KMS etcd di AKS dalam dokumentasi Microsoft Azure.

Simpan rahasia di Azure Key Vault

Untuk menghindari penyimpanan nilai sensitif sebagai rahasia Kubernetes di etcd sama sekali, gunakan penyedia Azure Key Vault untuk Driver CSI Secrets Store untuk memasang rahasia, kunci, dan sertifikat dari Azure Key Vault ke pod saat runtime. Untuk informasi selengkapnya, lihat penyedia Azure Key Vault untuk Driver CSI Secrets Store di dokumentasi Microsoft Azure.

Sifat jangkauan untuk cluster Layanan Azure Kubernetes

Berikut adalah ciri-ciri jangkauan untuk cluster Layanan Azure Kubernetes dan langkah-langkah remediasi yang disarankan.

Cluster Layanan Azure Kubernetes memungkinkan akses publik

Server API adalah titik akhir yang Anda gunakan untuk berkomunikasi dengan bidang kontrol Kubernetes cluster Anda. Cluster dapat dijangkau dari internet ketika titik akhir server API bersifat publik, atau ketika beban kerja diekspos melalui penyeimbang beban publik atau masuk. Titik akhir publik meningkatkan permukaan serangan Anda dan risiko akses tidak sah ke server API Kubernetes Anda. Penyerang berpotensi mengakses atau memodifikasi sumber daya cluster dan membaca data sensitif. Mengikuti praktik terbaik keamanan, batasi akses ke server API cluster dan beban kerja hanya untuk rentang IP yang diperlukan.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Batasi akses ke server API

Gunakan cluster pribadi sehingga server API hanya dapat dijangkau dari dalam jaringan virtual Anda, atau konfigurasikan rentang IP resmi untuk membatasi alamat sumber mana yang dapat mencapai

titik akhir server API publik. Untuk informasi selengkapnya, lihat Cluster Layanan Kubernetes Azure Pribadi di dokumentasi Microsoft Azure.

Batasi paparan publik dari beban kerja

Tinjau layanan yang diekspos melalui penyeimbang beban publik atau masuk, dan batasi atau hapus paparan publik jika tidak diperlukan. Gunakan penyeimbang beban internal, aturan grup keamanan jaringan, dan firewall aplikasi web pada titik masuk terkontrol untuk beban kerja yang harus dijangkau dari internet. Untuk informasi selengkapnya, lihat Konsep jaringan untuk AKS dalam dokumentasi Microsoft Azure.

Memperbaiki eksposur untuk pengguna Azure Graph

AWS Security Hub dapat menghasilkan temuan eksposur untuk pengguna Azure Graph.

Pada konsol Hub Keamanan, pengguna Azure Graph yang terlibat dalam temuan eksposur dan informasi pengidentifikasinya tercantum di bagian Sumber daya dari detail temuan. Secara terprogram, Anda dapat mengambil detail sumber daya dengan pen GetFindingsV2 goperasian Security Hub CSPM API.

Setelah mengidentifikasi sumber daya yang terlibat dalam penemuan eksposur, Anda dapat menghapus sumber daya jika Anda tidak membutuhkannya. Menghapus sumber daya yang tidak penting dapat mengurangi profil dan AWS biaya eksposur Anda. Jika sumber daya penting, ikuti langkah-langkah remediasi yang disarankan ini untuk membantu mengurangi risiko. Topik remediasi dibagi berdasarkan jenis sifat.

Temuan eksposur tunggal berisi masalah yang diidentifikasi dalam beberapa topik remediasi. Sebaliknya, Anda dapat mengatasi temuan eksposur dan menurunkan tingkat keparahannya dengan menangani hanya satu topik remediasi. Pendekatan Anda terhadap remediasi risiko tergantung pada persyaratan dan beban kerja organisasi Anda.

> **Note**
>
> Panduan remediasi yang disediakan dalam topik ini mungkin memerlukan konsultasi tambahan di sumber daya Microsoft Azure lainnya.

Daftar Isi

- Sifat kesalahan konfigurasi untuk pengguna Azure Graph

- Peran yang terkait dengan pengguna Azure Graph memiliki penetapan peran akses administratif
- Pengguna Azure Graph tidak mengaktifkan MFA

Sifat kesalahan konfigurasi untuk pengguna Azure Graph

Berikut adalah sifat kesalahan konfigurasi untuk pengguna Azure Graph dan langkah-langkah remediasi yang disarankan.

Peran yang terkait dengan pengguna Azure Graph memiliki penetapan peran akses administratif

Pengguna Azure Graph memiliki penetapan peran kontrol akses berbasis peran Azure (Azure RBAC) administratif, seperti`Owner`,, atau. `Contributor` `User Access Administrator` Penugasan sering berada pada ruang lingkup yang luas, seperti langganan atau kelompok manajemen. Penetapan peran administratif memberikan izin yang luas, sehingga penyerang dapat menggunakan akun pengguna yang dikompromikan untuk bergerak secara lateral, mengakses data, atau memanipulasi sumber daya di seluruh lingkungan Anda. Mengikuti prinsip-prinsip keamanan standar, berikan hak istimewa terkecil dan batasi penetapan peran administrator yang memiliki hak istimewa.

Remediasi

Lakukan satu atau beberapa tindakan berikut untuk mengatasi eksposur ini:

Meninjau dan mengidentifikasi penugasan peran administratif

Di portal Azure, tinjau penugasan peran pengguna. Cari peran administrator istimewa seperti`Owner`,, atau `Contributor` `User Access Administrator`, dan untuk peran khusus yang menggunakan wildcard (`*`) di dalamnya. `Actions` Untuk informasi selengkapnya, lihat Daftar penetapan peran Azure di dokumentasi Microsoft Azure.

Terapkan akses hak akses paling rendah

Hapus penetapan peran istimewa yang tidak perlu dan ganti dengan peran bawaan yang paling tidak memiliki hak istimewa, yang ditetapkan pada lingkup tersempit. Lebih suka peran fungsi pekerjaan daripada peran administrator istimewa. Pertahankan jumlah pemilik langganan seminimal mungkin — Microsoft merekomendasikan tidak lebih dari tiga.

Tetapkan peran ke grup, bukan pengguna individu. Gunakan Manajemen Identitas Privileged Microsoft Entra untuk membuat peran istimewa memenuhi syarat untuk aktivasi just-in-time dan terikat waktu alih-alih memberikan akses tetap. Untuk informasi selengkapnya, lihat Praktik terbaik untuk Azure RBAC di dokumentasi Microsoft Azure.

Pengguna Azure Graph tidak mengaktifkan MFA

Pengguna Azure Graph dapat masuk secara interaktif tanpa otentikasi multifaktor (MFA). Tanpa MFA, akun hanya dilindungi oleh kata sandi, yang membuatnya rentan terhadap serangan phishing, semprotan kata sandi, dan pengisian kredensial. Satu kata sandi yang dikompromikan sudah cukup bagi penyerang untuk masuk. Mengikuti prinsip keamanan standar, mewajibkan MFA untuk semua pengguna dengan login interaktif.

Remediasi: Memerlukan otentikasi multifaktor

Memerlukan MFA untuk pengguna melalui kebijakan Akses Bersyarat Microsoft Entra. Untuk cakupan yang luas, aktifkan default keamanan atau kebijakan Akses Bersyarat yang memerlukan MFA untuk semua pengguna. Prioritaskan kebijakan khusus untuk administrator.

Jika memungkinkan, mintalah metode anti phishing — seperti kunci keamanan FIDO2, kunci sandi, atau Windows Hello for Business — melalui kekuatan otentikasi Akses Bersyarat. Hindari mengizinkan metode yang mudah rusak seperti SMS atau suara. Untuk informasi selengkapnya, lihat Merencanakan penyebaran otentikasi multifaktor dalam dokumentasi Microsoft Azure.

Memahami temuan akses yang tidak digunakan di Hub Keamanan

Security Hub menggunakan IAM Access Analyzer untuk mengidentifikasi izin, peran, kunci akses, dan kata sandi IAM yang tidak digunakan di akun Anda. Temuan ini membantu Anda menerapkan praktik terbaik keamanan akses hak istimewa terendah dengan menyoroti prinsip-prinsip dan izin IAM yang tidak digunakan secara aktif. Kemampuan ini disediakan untuk semua pelanggan Security Hub tanpa biaya tambahan.

Cara kerja analisis akses yang tidak digunakan

Saat Anda mengaktifkan Hub Keamanan, layanan secara otomatis membuat Penganalisis Akses IAM yang ditautkan ke layanan di akun Anda. Penganalisis ini mengevaluasi semua prinsipal IAM (peran dan pengguna) terhadap data AWS CloudTrail aktivitas untuk menentukan prinsip dan izin mana yang belum digunakan dalam periode lookback 90 hari. Periode lookback tidak dapat dikonfigurasi.

IAM Access Analyzer mengevaluasi kembali semua temuan aktif setiap 24 jam. Ketika prinsipal atau izin yang sebelumnya tidak digunakan menjadi aktif, temuan yang sesuai diselesaikan secara otomatis.

Penganalisis akses yang tidak digunakan berjalan di AS Timur (Virginia Utara) karena IAM adalah layanan global. Security Hub mereplikasi temuan ke semua Wilayah tempat Anda mengaktifkan

Hub Keamanan. Anda tidak perlu mengaktifkan Hub Keamanan di AS Timur (Virginia Utara) agar penganalisis dapat berjalan.

Jenis pencarian akses yang tidak digunakan

Security Hub menghasilkan empat jenis temuan akses yang tidak digunakan:

Tipe temuan	Deskripsi	Sumber daya dievaluasi
Tidak Digunakan DiamRole	Peran IAM yang belum diasumsikan dalam periode lookback 90 hari.	IAM Role
UnusedIAM UserAccessKey	Kunci akses pengguna IAM yang belum digunakan untuk menandatangani permintaan API dalam periode lookback 90 hari.	Pengguna IAM
UnusedIAM UserPassword	Kata sandi pengguna IAM yang belum digunakan untuk masuk konsol dalam periode retrospektif 90 hari.	Pengguna IAM
UnusedPermission	Tindakan IAM tertentu yang diberikan kepada peran atau pengguna tetapi belum dipanggil dalam periode lookback 90 hari.	Peran IAM atau pengguna IAM

Service-linked penganalisis

Penganalisis Akses IAM yang dibuat oleh Security Hub adalah penganalisis terkait layanan. Anda dapat melihatnya di konsol IAM Access Analyzer, tetapi Anda tidak dapat memodifikasi atau menghapusnya saat Security Hub diaktifkan.

Saat Anda menonaktifkan Hub Keamanan di semua Wilayah, penganalisis terkait layanan akan dihapus secara otomatis. Jika penghapusan otomatis gagal, Anda dapat menghapus penganalisis dengan memanggil operasi `DeleteServiceLinkedAnalyzer` API Penganalisis Akses IAM. Operasi ini berhasil hanya setelah Hub Keamanan sepenuhnya dinonaktifkan untuk akun Anda.

Penganalisis terkait layanan terpisah dari penganalisis yang dikelola pelanggan yang mungkin telah Anda buat secara independen di IAM Access Analyzer. Membuat atau menghapus penganalisis yang dikelola pelanggan tidak memengaruhi penganalisis terkait layanan, dan sebaliknya.

Melihat temuan akses yang tidak digunakan

Temuan akses yang tidak digunakan muncul di konsol Hub Keamanan bersama temuan Hub Keamanan lainnya. Anda dapat memfilter temuan berdasarkan jenis untuk hanya melihat temuan akses yang tidak digunakan. Temuan akses yang tidak digunakan diformat dalam Open Cybersecurity Schema Framework (OCSF), format yang sama yang digunakan oleh semua temuan Security Hub.

Untuk UnusedPermission temuan, jika Anda menghapus beberapa izin yang tidak digunakan dari kebijakan yang terlalu permisif, tetapi tidak semua, Security Hub menutup temuan yang ada dan membuat temuan baru untuk kebijakan yang direvisi jika masih terlalu permisif.

Temuan akses yang tidak digunakan juga dapat diakses dari konsol Penganalisis Akses IAM. Temuan akses yang tidak digunakan di konsol Penganalisis Akses IAM hanya dapat dibaca dan hanya terlihat di wilayah AS Timur (Virginia Utara).

Akses yang tidak digunakan dalam temuan eksposur

Informasi akses yang tidak digunakan dapat muncul sebagai sifat kontekstual dalam temuan eksposur Security Hub. Ketika peran IAM yang dilampirkan ke sumber daya memiliki izin yang tidak digunakan, temuan eksposur menyertakan ini sebagai konteks tambahan. Ini membantu Anda memahami potensi radius ledakan kerentanan — sumber daya dengan peran IAM yang terlalu istimewa menghadirkan risiko lebih tinggi daripada sumber daya dengan hak istimewa terendah.

Jenis sumber daya berikut dapat menampilkan sifat kontekstual akses yang tidak digunakan dalam temuan eksposur mereka:

- Instans Amazon Elastic Compute Cloud
- AWS Lambda fungsi
- Layanan Amazon Elastic Container Service
- Cluster Layanan Amazon Elastic Kubernetes
- Pengguna IAM (langsung)

Untuk informasi lebih lanjut tentang temuan paparan, lihatTemuan paparan di Security Hub.

Rekomendasi kebijakan untuk izin yang tidak digunakan

Untuk UnusedPermission temuan, Security Hub dapat menghasilkan rekomendasi kebijakan hak istimewa terkecil. Rekomendasi ini menunjukkan kepada Anda kebijakan penggantian dengan cakupan yang hanya mempertahankan izin yang sebenarnya digunakan kepala sekolah Anda. Untuk informasi selengkapnya, lihat Menghasilkan rekomendasi kebijakan untuk temuan akses yang tidak digunakan.

Harga

Penganalisis Akses IAM yang terhubung dengan layanan disediakan untuk semua pelanggan Hub Keamanan tanpa biaya tambahan. Anda tidak dikenakan biaya terpisah untuk penganalisis atau untuk temuan akses yang tidak digunakan.

Menghasilkan rekomendasi kebijakan untuk temuan akses yang tidak digunakan

Untuk temuan izin yang tidak terpakai, Security Hub dapat menghasilkan rekomendasi kebijakan hak istimewa terkecil yang menunjukkan kebijakan penggantian dengan cakupan. Rekomendasi mengevaluasi setiap kebijakan yang dilampirkan pada prinsipal IAM dan menghasilkan pengganti yang hanya mempertahankan izin yang sebenarnya digunakan oleh kepala sekolah. Kemampuan ini disediakan untuk semua pelanggan Security Hub tanpa biaya tambahan.

Bagaimana rekomendasi kebijakan bekerja

Pembuatan rekomendasi kebijakan adalah operasi asinkron. Untuk menghasilkan dan mengambil rekomendasi:

1. Ambil temuan izin yang tidak digunakan dari Hub Keamanan menggunakan operasi `GetFindingsV2` API. Perhatikan `metadata.uid` bidang dari temuan.
2. Hu `GenerateRecommendedPolicyV2` bungi temuan itu`metadata.uid`. Ini memulai pembuatan rekomendasi, yang biasanya selesai dalam 20 detik.
3. Jajak pendapat `GetRecommendedPolicyV2` dengan yang sama `metadata.uid` sampai `status` bidang kembali`SUCCEEDED`.
4. Tanggapan berisi satu atau lebih langkah rekomendasi. Setiap langkah menentukan `recommendedAction` salah satu `CREATE_POLICY` (membuat dan melampirkan kebijakan

penggantian dengan cakupan) atau `DETACH_POLICY` (lepaskan kebijakan asli yang terlalu istimewa). Untuk `CREATE_POLICY` langkah-langkah, respons mencakup `existingPolicy` JSON dan `recommendedPolicy` JSON sehingga Anda dapat membandingkannya.

Anda harus menelepon `GenerateRecommendedPolicyV2` sebelum `GetRecommendedPolicyV2` menelepon jika rekomendasi belum dibuat sebelumnya untuk temuan itu.

Siapa yang bisa menghasilkan rekomendasi

Baik pemilik akun maupun administrator yang didelegasikan dapat memanggil operasi API ini:

- Pemilik akun dapat membuat dan melihat rekomendasi untuk temuan izin yang tidak digunakan di akun mereka sendiri.
- Administrator yang didelegasikan dapat membuat dan melihat rekomendasi untuk temuan izin akun anggota yang tidak terpakai dalam organisasi mereka.

Jika Anda bukan administrator yang didelegasikan dan temuan tersebut milik akun yang berbeda, operasi API mengembalikan `AccessDeniedException` kesalahan.

Siklus hidup rekomendasi

- Rekomendasi disimpan dalam cache selama 90 hari dan tetap tersedia selama temuan aktif (tidak Ditutup). Namun, memanggil `GenerateRecommendedPolicyV2` beberapa kali membatalkan cache dan memulai pekerjaan baru yang menggantikan kebijakan cache. Panggil `GenerateRecommendedPolicyV2` hanya sekali per temuan.
- Rekomendasi mengikuti pola lepas-dan-pasang. Itu tidak mengubah kebijakan IAM Anda yang ada. Anda meninjau kebijakan yang disarankan dan menerapkannya secara manual di konsol IAM atau melalui IAM API.
- Jika temuan diselesaikan (misalnya, karena izin yang sebelumnya tidak digunakan sekarang digunakan), rekomendasi tidak lagi tersedia.

Kasus kesalahan

Operasi API mengembalikan kesalahan dalam situasi berikut:

- Temuan telah diselesaikan - `InvalidInputException` (HTTP 400).

- Temuan ini bukan temuan izin yang tidak digunakan - `InvalidInputException` (HTTP 400).
- Prinsip IAM dibuat melalui kumpulan izin Pusat Identitas IAM. Kebijakan untuk prinsipal kumpulan izin tidak dapat dimodifikasi secara langsung. Rekomendasi mengembalikan `FAILED` status dengan penjelasan.
- Penelepon bukan administrator yang didelegasikan dan temuan itu milik akun yang berbeda - `AccessDeniedException` (HTTP 403).
- Belum ada rekomendasi yang dibuat dan Anda menelepon `GetRecommendedPolicyV2` tanpa menelepon `GenerateRecommendedPolicyV2` terlebih dahulu - `ResourceNotFoundException` (HTTP 404).

Menggunakan konsol

Di konsol Hub Keamanan, Anda dapat membuat rekomendasi kebijakan dengan melihat pencarian izin yang tidak digunakan dan memilih tab Remediasi. Konsol menampilkan pemintal pemuatan saat rekomendasi sedang dibuat. Ketika rekomendasi sudah siap, Anda dapat memilih Prat injau untuk melihat perbandingan berdampingan dari kebijakan Anda saat ini dan penggantian hak istimewa terendah yang disarankan. Anda dapat menyalin kebijakan yang disarankan dalam format JSON.

Referensi API

- GenerateRecommendedPolicyV2— Memulai pembuatan asinkron dari rekomendasi kebijakan hak istimewa terkecil untuk temuan izin yang tidak digunakan. Mengambil temuan `metadata.uid` sebagai masukan. Mengembalikan HTTP 200 dengan tubuh kosong saat berhasil.
- GetRecommendedPolicyV2— Mengambil rekomendasi kebijakan yang dihasilkan. Mengambil temuan `metadata.uid` sebagai masukan. Mendukung pagination dengan `maxResults` (1—100) dan `nextToken` parameter. Mengembalikan status rekomendasi (`IN_PROGRESS`,`SUCCEEDED`, atau`FAILED`), langkah-langkah rekomendasi, ARN sumber daya, dan kesalahan apa pun.

Untuk dokumentasi API terperinci, lihat Referensi API Hub Keamanan.

Pemindaian Jaringan di Hub Keamanan

Pemindaian Jaringan adalah fitur opt-in dari Security Hub yang melakukan pengujian jangkauan jaringan aktif pada sumber daya cloud Anda. Control-plane analisis mengevaluasi grup keamanan, Daftar Kontrol Akses Jaringan (NACL), dan tabel rute untuk menentukan apa yang dapat dijangkau.

Pemindaian jaringan melangkah lebih jauh dengan mendeteksi apa yang sebenarnya dapat dijangkau. Ini menyelidiki sumber daya Anda dari luar akun Anda untuk mengidentifikasi port terbuka dan layanan yang sedang berjalan.

Semua pemindaian berasal AWS dari alamat IP yang dimiliki dan menjawab dua pertanyaan: Apakah sumber daya ini dapat dijangkau dari internet? Jika dapat dijangkau, apa yang sedang berjalan? Pemindaian Jaringan menerbitkan hasil sebagai temuan OCSF mandiri di Security Hub dengan bukti pemindaian.

Jenis sumber daya yang didukung

Pemindaian Jaringan mendukung jenis sumber daya berikut.

Penyedia cloud	Tipe sumber daya
AWS	Instans EC2 (dengan IP publik)
AWS	IP elastis (EIP)
AWS	Penyeimbang Beban Jaringan (NLB)
AWS	Penyeimbang Beban Aplikasi (ALB)
AWS	Penyeimbang Beban Klasik (CLB)
Biru langit	Alamat IP Publik

> **Note**
>
> Pemindaian Jaringan memindai setiap jenis sumber daya secara independen. Untuk penyeimbang beban, Pemindaian Jaringan menyelesaikan dan memindai nama DNS. Pemindaian Jaringan hanya memindai instans EC2 individual di belakang penyeimbang beban jika mereka memiliki IP publik atau EIP mereka sendiri.

Aktifkan Pemindaian Jaringan

Untuk mengaktifkan Pemindaian Jaringan, Hub Keamanan harus diaktifkan di akun Anda. Anda dapat mengaktifkan Pemindaian Jaringan melalui kebijakan konfigurasi atau untuk akun individual.

Akun organisasi (disarankan) — Aktifkan Pemindaian Jaringan di seluruh akun dan Wilayah organisasi Anda dengan membuat atau mengedit kebijakan konfigurasi. Untuk informasi selengkapnya tentang mengedit kebijakan konfigurasi, lihat Mengedit kebijakan konfigurasi. Ketika Pemindaian Jaringan diaktifkan melalui kebijakan konfigurasi, akun anggota tidak dapat mematikan fitur tersebut.

Akun individu — Untuk akun yang tidak dikelola oleh kebijakan konfigurasi, Anda dapat mengaktifkan Pemindaian Jaringan menggunakan salah satu metode berikut.

> **Note**
>
> Dengan mengaktifkan Pemindaian Jaringan, Anda mengotorisasi Hub Keamanan untuk melakukan pemindaian jaringan aktif terhadap sumber daya di AWS lingkungan dan lingkungan Azure Anda. Ini termasuk upaya koneksi port TCP, identifikasi aplikasi dan protokol, dan pengumpulan spanduk layanan, header HTTP, dan metadata sertifikat TLS.

Security Hub console

Untuk mengaktifkan Pemindaian Jaringan

1. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Di panel navigasi, pilih Peng aturan umum.
3. Temukan bagian Pemindaian Jaringan.
4. Pilih Aktifkan.
5. Konfirmasikan otorisasi untuk melanjutkan pemindaian jaringan aktif.

Security Hub API

Memanggil `EnableSecurityHubFeatureV2` API dengan nama `NETWORK_SCANNING` fitur.

> **Note**
>
> Memanggil API ini saat Pemindaian Jaringan sudah diaktifkan mengembalikan respons 200. Layanan mempertahankan stempel `UpdatedAt` waktu dari pengaktifan asli.

AWS CLI

Jalankan perintah berikut untuk mengaktifkan Pemindaian Jaringan:

```
aws securityhub enable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Cara kerja Pemindaian Jaringan

Setelah Anda mengaktifkan Pemindaian Jaringan, hal berikut terjadi:

- Pemindaian Jaringan memindai sumber daya yang ada dalam waktu sekitar 24 jam setelah mengaktifkan fitur.
- Pemindaian Jaringan memindai sumber daya baru segera setelah Hub Keamanan menerima pemberitahuan sumber daya yang dibuat.
- Pemindaian Jaringan memindai ulang sumber daya saat perubahan bidang kontrol tertentu yang memenuhi syarat dilakukan pada sumber daya yang memenuhi syarat pemindaian.
- Pemindaian Jaringan memindai ulang sumber daya aktif kira-kira setiap 12 jam untuk mendeteksi perubahan jangkauan.

Sumber daya fana atau berumur pendek mungkin tidak dipindai sebelum dihentikan.

Temuan Pemindaian Jaringan

Pemindaian Jaringan menerbitkan temuan dalam format Open Cybersecurity Schema Framework (OCSF), menggunakan Ek AWS stensi OCSF, dan mereka muncul bersama temuan Hub Keamanan lainnya. Pemindaian Jaringan membuat temuan apakah sumber daya memiliki port yang dapat dijangkau atau tidak. Jika temuan tidak ada untuk jenis sumber daya yang didukung, Pemindaian Jaringan belum memindai sumber daya.

Temuan untuk port yang dapat dijangkau

Setiap temuan mewakili satu port yang dapat dijangkau pada kombinasi sumber daya dan alamat tertentu. `port_scan_result_list`Bagian dari temuan OCSF berisi hasil pemindaian. Contoh berikut menunjukkan informasi yang dikembalikan untuk sumber daya yang dapat dijangkau:

```
"port_scan_result_list": [
    {
      "port_info": {
        "port": 6379,
        "protocol_name": "tcp",
        "protocol_num": 6
      },
      "status": "Open",
      "status_id": 1,
      "svc_name": "redis"
    }
],
```



```
"port_scan_result_list": [
    {
      "http_response": {
        "code": 200,
        "content_type": "text/html; charset=UTF-8",
        "http_headers": [
          {
            "name": "Server",
            "value": "Apache/2.4.68 (Amazon Linux)"
          },
          {
            "name": "Content-Type",
            "value": "text/html; charset=UTF-8"
          }
        ],
        "latency": 124
      },
      "port_info": {
        "port": 8080,
        "protocol_name": "tcp",
        "protocol_num": 6
      },
      "status": "Open",
      "status_id": 1
    }
  ],
```

Temuan informasi untuk tidak ada port terbuka

Pemindaian Jaringan menciptakan temuan ketika mendeteksi tidak ada port terbuka pada sumber daya. Temuan ini memiliki tingkat keparahan `Informational` dan tidak memerlukan tindakan. Ini menegaskan bahwa Pemindaian Jaringan memindai sumber daya.

Temuan Informasi tetap terbuka di Hub Keamanan sampai Anda menghapus sumber daya atau hingga Pemindaian Jaringan mendeteksi port terbuka pada sumber daya. Ketika Pemindaian Jaringan mengidentifikasi port terbuka pada sumber daya dengan temuan Informasi, itu menutup temuan Informasi. Ini kemudian menciptakan temuan untuk setiap port terbuka.

Temuan informasi untuk tidak ada port terbuka mencakup port yang didukung Pemindaian Jaringan saat ini. Untuk daftar port yang didukung, lihatthe section called “Port yang didukung”.

Menemukan peristiwa siklus hidup

Tabel berikut menjelaskan siklus hidup untuk temuan Pemindaian Jaringan.

Peristiwa	Apa yang terjadi
Tidak ada port terbuka yang terdeteksi	Pemindaian Jaringan menciptakan `Informational` temuan yang tidak memerlukan tindakan
Buka port terdeteksi pada sumber daya dengan Temuan Informasi	Pemindaian Jaringan menutup temuan Informasi dan membuat temuan untuk setiap port terbuka
Port pertama kali terdeteksi sebagai dapat dijangkau	Pemindaian Jaringan membuat dan menerbitkan temuan baru
Port masih dapat dijangkau saat scan ulang (tidak ada perubahan)	Pemindaian Jaringan secara berkala menyegarkan temuan
Pelabuhan masih dapat dijangkau tetapi bukti berubah	Pemindaian Jaringan merepresentasikan temuan dengan bukti terbaru
Pelabuhan tidak lagi dapat dijangkau	Penemuan tetap terbuka sampai pemindaian ulang berikutnya mengonfirmasi bahwa port tidak dapat dijangkau

Peristiwa	Apa yang terjadi
Sumber daya dihentikan atau dihapus	Pemindaian Jaringan menutup semua temuan untuk sumber daya dengan menyetel `activity_name` atribut ke `Close`
Alamat IP dihapus dari sumber daya	Pemindaian Jaringan menutup temuan untuk IP tertentu
Pemindaian Jaringan dinonaktifkan	Pemindaian Jaringan tidak menghasilkan temuan baru; temuan yang ada tetap ada sampai mereka menua
Hub Keamanan dinonaktifkan	Anda tidak lagi memiliki akses ke temuan

Jika port dapat dijangkau sebentar-sebentar, Pemindaian Jaringan mendasarkan temuan pada bukti positif pada waktu pemindaian. Setelah Anda memperbaiki masalah (misalnya, dengan menutup aturan firewall atau menghentikan layanan), Pemindaian Jaringan menutup temuan pada pemindaian berikutnya.

Menonaktifkan Pemindaian Jaringan tidak segera menutup temuan. Temuan yang ada tetap terlihat sampai mereka menua melalui siklus hidup penemuan Hub Keamanan normal.

> **Note**
>
> Saat Anda melampirkan alamat IP Elastic (EIP) ke instans Amazon EC2, Pemindaian Jaringan menghasilkan temuan pada sumber daya EIP. EIP adalah sumber daya IP tingkat atas yang memiliki alamat. Untuk sumber daya Network Load Balancer (NLB), nama DNS dan EIP terlampir adalah titik masuk jaringan yang berbeda, sehingga Pemindaian Jaringan menghasilkan temuan terpisah untuk masing-masing.

Pindai bukti

Ketika Pemindaian Jaringan mendeteksi bahwa port dapat dijangkau, temuan tersebut mencakup bukti tentang layanan yang dapat dijangkau. Jenis bukti berikut dapat dikumpulkan:

Spanduk TCP

Byte awal dikirim oleh layanan pada koneksi, seperti string versi SSH.

Metadata HTTP

Header respons dan kode status HTTP.

Sertifikat TLS

Nama Umum (CN), penerbit, tanggal kedaluwarsa, dan status yang ditandatangani sendiri.

Deteksi Layanan

Aplikasi atau protokol yang diidentifikasi berjalan di port.

Mengecualikan sumber daya dari pemindaian

Untuk mengecualikan sumber daya dari Pemindaian Jaringan, tambahkan kunci tag `SecurityHubNetworkScanExclusion` ke sumber daya. Nilai tag bisa berupa nilai apa saja atau kosong.

Anda harus menerapkan tag ke sumber daya aktual dengan IP publik yang dapat dipindai:

- Untuk EIP yang dilampirkan ke instance EC2 — beri tag pada EIP, bukan instance EC2.
- Untuk instance EC2 dengan hanya IP publik (tanpa EIP) — beri tag instance EC2.
- Untuk penyeimbang beban — beri tag penyeimbang beban dan target apa pun dengan IP publik individu.

Saat Anda menambahkan tag pengecualian, Pemindaian Jaringan menghentikan pemindaian di masa mendatang dan menutup temuan aktif untuk sumber daya tersebut. Menghapus tag membuat sumber daya memenuhi syarat untuk pemindaian lagi.

Port yang didukung

Pemindaian Jaringan memindai port TCP terkenal berikut pada sumber daya yang memenuhi syarat.

```
21, 22, 23, 25, 53, 80, 110, 143, 443, 445, 1433, 3306, 3389, 5432,
5900, 6379, 8080, 8443, 9200, 27017
```

Multi-cloud dukungan

Pemindaian Jaringan mendukung Alamat IP Publik Azure. Untuk memindai sumber daya Azure, buat konektor Hub Keamanan ke lingkungan Azure Anda. Untuk informasi selengkapnya tentang

mengintegrasikan dengan Microsoft Azure, lihat Mengintegrasikan Hub Keamanan dengan Microsoft Azure.

Perilaku pemindaian, bukti, dan temuan untuk sumber daya Azure identik dengan AWS sumber daya. Temuan muncul bersamaan dengan AWS temuan dengan penyedia cloud dan metadata wilayah yang sesuai.

Ketersediaan wilayah

Pemindaian Jaringan tersedia di Wil AWS ayah komersial di mana Hub Keamanan tersedia.

Nonaktifkan Pemindaian Jaringan

Jika organisasi Anda menggunakan kebijakan konfigurasi, administrator yang didelegasikan dapat menonaktifkan Pemindaian Jaringan di seluruh akun dan Wilayah tertentu dengan mengedit kebijakan konfigurasi. Untuk informasi selengkapnya tentang mengedit kebijakan konfigurasi, lihat Mengedit kebijakan konfigurasi. Saat mengedit kebijakan, pilih kemampuan Pemindaian Jaringan, pilih N onaktifkan, lalu tentukan akun dan Wilayah tempat Anda ingin menonaktifkan pemindaian.

Untuk akun yang tidak dikelola oleh kebijakan konfigurasi, Anda dapat menonaktifkan Pemindaian Jaringan menggunakan salah satu metode berikut.

Security Hub console

Untuk menonaktifkan Pemindaian Jaringan

1. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Di panel navigasi, pilih Peng aturan umum.
3. Temukan bagian Pemindaian Jaringan.
4. Pilih Disable (Nonaktifkan).
5. Konfirmasikan bahwa Anda ingin menonaktifkan Pemindaian Jaringan.

Security Hub API

Memanggil `DisableSecurityHubFeatureV2` API dengan nama `NETWORK_SCANNING` fitur.

AWS CLI

Jalankan perintah berikut untuk menonaktifkan Pemindaian Jaringan:

```
aws securityhub disable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

Saat Anda menonaktifkan Pemindaian Jaringan:

- Pemindaian Jaringan tidak memicu pemindaian baru.
- Temuan yang ada tetap terlihat sampai mereka menua melalui siklus hidup penemuan Hub Keamanan normal.
- Pemindaian Jaringan menyelesaikan semua pemindaian yang sudah berlangsung.

Otomatisasi di Hub Keamanan

Security Hub menyertakan fitur yang secara otomatis memodifikasi dan mengambil tindakan atas temuan berdasarkan spesifikasi Anda.

Security Hub saat ini mendukung jenis otomatisasi berikut:

- Aturan otomatisasi — Secara otomatis memperbarui dan menekan temuan, serta mengirim temuan ke alat tiket, hampir secara real time berdasarkan kriteria yang ditentukan.
- Respon dan remediasi otomatis — Buat EventBridge aturan Amazon khusus yang menentukan tindakan otomatis yang harus diambil terhadap temuan dan wawasan tertentu.

Aturan otomatisasi sangat membantu ketika Anda ingin memperbarui bidang pencarian secara otomatis di Open Cybersecurity Schema Framework (OCSF). Misalnya, Anda dapat menggunakan aturan otomatisasi untuk memperbarui tingkat keparahan temuan untuk sumber daya dengan tag tertentu. Menggunakan aturan otomatisasi menghilangkan kebutuhan untuk memperbarui tingkat keparahan secara manual dari setiap temuan yang terkait dengan tag tertentu. Anda dapat mengonfigurasi aturan otomatisasi untuk membuat tiket di alat seperti Jira Cloud dan ServiceNow ketika temuan cocok dengan atribut tertentu. Tiket dibuat dari temuan segera setelah tiba di Security Hub.

EventBridge aturan berguna ketika Anda ingin mengambil tindakan di luar Hub Keamanan untuk temuan tertentu atau mengirim temuan khusus ke alat pihak ketiga untuk remediasi atau penyelidikan tambahan. Aturan dapat digunakan untuk memicu tindakan yang didukung, seperti memanggil AWS Lambda fungsi atau memberi tahu topik Amazon Simple Notification Service (Amazon SNS) tentang temuan tertentu.

Aturan otomatisasi berlaku sebelum EventBridge aturan diterapkan. Artinya, aturan otomatisasi dipicu dan memperbarui temuan sebelum EventBridge menerima temuan. EventBridge aturan kemudian berlaku untuk temuan yang diperbarui.

Aturan otomatisasi di Hub Keamanan

Dengan Security Hub, Anda dapat mengotomatiskan tugas seperti memperbarui rincian pencarian dan membuat tiket untuk integrasi pihak ketiga.

Aturan otomatisasi dan Wilayah AWS

Aturan otomatisasi dapat dibuat dalam satu Wilayah AWS dan kemudian diterapkan di semua yang dikonfigurasi Wilayah AWS. Saat menggunakan agregasi Wilayah, Anda hanya dapat membuat aturan di Wilayah rumah. Saat membuat aturan di Wilayah beranda, aturan apa pun yang Anda tetapkan diterapkan ke semua Wilayah yang ditautkan, kecuali kriteria aturan Anda mengecualikan Wilayah tertaut tertentu. Anda harus membuat aturan otomatisasi untuk Wilayah mana pun yang bukan Wilayah tertaut.

Tindakan aturan dan kriteria

Aturan otomatisasi di Hub Keamanan menggunakan kriteria untuk mereferensikan atribut OCSF dalam temuan Hub Keamanan. Misalnya, filter yang didukung untuk `Criteria` parameter dalam CreateAutomationRuleV2 cocok dengan filter yang didukung untuk `Filters` parameter di GetFindings V2. Ini berarti filter yang digunakan dalam aturan otomatisasi dapat digunakan untuk mendapatkan temuan. Security Hub mendukung bidang OCSF berikut untuk kriteria aturan otomatisasi.

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
`activity_id`	`Activity ID`	`Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)`	`Number`
`activity_name`	`Provider status`	`EQUALS, PREFIX, CONTAINS, NOT_EQUAL`	`String`

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
		S, PREFIX_NO T_EQUALS	
class_name	Finding class name	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
cloud.acc ount.name	Finding account name	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
cloud.acc ount.uid	Account ID	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
cloud.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String
cloud.region	Region	EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
compliance.assessments.category	Assessment category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.assessments.meets_criteria	Compliance assessment meets criteria	True, False	Boolean
compliance.assessments.name	Assessment name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control	Security control ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.control_parameters	Control parameter name	EQUALS	Map
compliance.standards	Applicable standards	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
compliance.status	Compliance status	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
compliance.status_id	Compliance status ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
confidence_score	Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.created_time_dt	Created at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.desc	Finding description	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.first_seen_time_dt	First observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
finding_info.last_seen_time_dt	Last observed at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.modified_time_dt	Updated at	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
finding_info.related_events.product.uid	Related findings product ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.title	Related findings title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.traits.category	Traits category	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.related_events.uid	Related findings ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
finding_info.related_events_count	Related findings count	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
finding_info.src_url	Source URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.tags	Finding info tags	EQUALS	Map
finding_info.title	Finding title	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.types	Finding type	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
finding_info.uid	Provider finding ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
metadata.product.feature.uid	Generator ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.name	Product name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.uid	Product ARN	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
metadata.product.vendor_name	Company name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.desc	Recommendation text	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
remediation.references	Recommendation URL	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
resources.cloud_partition	Resource partition	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.modified_time_dt	Resource last modified time	Start, End, DateRange	Date (formatted as 2022-12-01T21:47:39.269Z)
resources.name	Resource name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.name	Account name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.account.uid	Account	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.owner.org.uid	Organization	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
resources.provider	Cloud provider	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.region	Resource region	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.tags	Resource tags	EQUALS	Map
resources.type	Resource type	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
resources.uid	Resource ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vendor_attributes.severity	Provider severity	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
vendor_attributes.severity_id	Provider severity ID	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
vulnerabilities.affected_code.file.path	Affected code file path	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.affected_packages.name	Affected package name	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.cve.cvss.base_score	CVE CVSS base score	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Number
vulnerabilities.cve.epss.score	Epss score	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.cve.uid	Vulnerability ID	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Bidang OCSF	Nilai filter konsol	Operator filter	Jenis bidang
vulnerabilities.fix_coverage	Software vulnerabilities coverage	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
vulnerabilities.is_exploit_available	Software vulnerabilities with exploit available	True, False	Boolean
vulnerabilities.is_fix_available	Software vulnerabilities with fix available	True, False	Boolean
vulnerabilities.related_vulnerabilities	Related vulnerabilities	EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Untuk kriteria berlabel sebagai bidang string, menggunakan operator filter yang berbeda pada bidang yang sama mempengaruhi logika evaluasi. Untuk informasi selengkapnya, lihat StringFilter Referensi API Hub Keamanan.

Setiap kriteria mendukung jumlah nilai maksimum yang dapat digunakan untuk menyaring temuan yang cocok. Untuk batas setiap kriteria, lihat OcsfFindingFilters di Referensi API Hub Keamanan

Bidang OCSF yang dapat diperbarui

Berikut ini adalah bidang OCSF yang dapat diperbarui menggunakan aturan otomatisasi.

- `Comment`
- `SeverityId`
- `StatusId`

Bagaimana aturan otomatisasi mengevaluasi temuan

Aturan otomatisasi mengevaluasi temuan baru dan terbaru yang dihasilkan atau diserap oleh Hub Keamanan setelah Anda membuat aturan.

Aturan otomatisasi mengevaluasi temuan asli yang disediakan penyedia. Penyedia dapat memberikan temuan baru dan memperbarui temuan yang ada melalui integrasi mereka dengan Security Hub. Aturan tidak dipicu saat Anda memperbarui bidang pencarian setelah pembuatan aturan melalui `BatchUpdateFindingsV2` operasi. Jika Anda membuat aturan otomatisasi dan membuat `BatchUpdateFindingsV2` pembaruan yang keduanya memengaruhi bidang pencarian yang sama, pembaruan terakhir menetapkan nilai untuk bidang tersebut. Ambil contoh berikut:

Anda gunakan `BatchUpdateFindingsV2` untuk memperbarui `Status` bidang temuan dari `New` ke`In Process`. Jika Anda memanggil`GetFindingsV2`, `Status` bidang sekarang memiliki nilai`In Process`. Anda membuat aturan otomatisasi yang mengubah `Status` bidang temuan dari `New` ke `Suppressed` (ingat bahwa aturan mengabaikan pembaruan yang dibuat dengan`BatchUpdateFindingsV2`). Penyedia temuan memperbarui temuan dan mengubah `Status` bidang menjadi`New`. Jika Anda memang `GetFindingsV2` gil, `Status` bidang sekarang memiliki nilai `Suppressed` karena aturan otomatisasi diterapkan, dan aturan tersebut adalah tindakan terakhir yang diambil pada temuan.

Saat Anda membuat atau mengedit aturan di konsol Hub Keamanan, konsol menampilkan pratinjau temuan yang sesuai dengan kriteria aturan. Sementara aturan otomatisasi mengevaluasi temuan asli yang dikirim oleh penyedia temuan, pratinjau konsol mencerminkan temuan dalam keadaan akhirnya seperti yang akan ditampilkan dalam respons terhadap operasi `GetFindingsV2` API (yaitu, setelah tindakan aturan atau pembaruan lain diterapkan pada temuan).

Bagaimana aturan otomatisasi diurutkan

Setiap aturan otomatisasi diberi urutan aturan. Ini menentukan urutan di mana Security Hub menerapkan aturan otomatisasi Anda, dan menjadi penting ketika beberapa aturan berhubungan dengan bidang temuan atau temuan yang sama.

Ketika beberapa tindakan aturan berhubungan dengan bidang temuan atau temuan yang sama, aturan dengan nilai numerik tertinggi untuk urutan aturan berlaku terakhir dan memiliki efek akhir.

Saat Anda membuat aturan di konsol Hub Keamanan, Hub Keamanan secara otomatis menetapkan urutan aturan berdasarkan urutan pembuatan aturan. Aturan pertama yang Anda buat akan memiliki urutan aturan 1. Ketika ada lebih dari satu aturan, setiap aturan yang dibuat selanjutnya akan memiliki nilai numerik tertinggi berikutnya yang tersedia untuk urutan aturan.

Saat Anda membuat aturan melalui CreateAutomationRuleV2 API atau AWS CLI, Security Hub menerapkan aturan dengan nilai numerik terendah untuk `RuleOrder` pertama. Kemudian menerapkan aturan berikutnya dalam urutan menaik. Jika beberapa temuan memiliki `RuleOrder` hal yang sama, Security Hub menerapkan aturan dengan nilai sebelumnya untuk `UpdatedAt` bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

Anda dapat mengubah urutan aturan kapan saja.

Contoh urutan aturan:

Aturan A (urutan aturan adalah**1**):

- Kriteria Aturan A
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type`adalah `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState`adalah `NEW`
  - `Workflow.Status` = `ACTIVE`
- Tindakan Aturan A
  - Perbarui `Confidence` ke `95`
  - Perbarui `Severity` ke `CRITICAL`
  - Perbarui `Comment` ke `This needs attention`

Aturan B (urutan aturan adalah**2**):

- Kriteria Aturan B
  - `AwsAccountId` = `123456789012`
- Tindakan Aturan B
  - Perbarui `Severity` ke `INFORMATIONAL`

Pertama, tindakan Aturan A berlaku untuk temuan Hub Keamanan yang cocok dengan kriteria Aturan A. Kemudian, tindakan Aturan B berlaku untuk temuan Hub Keamanan dengan ID akun yang ditentukan. Dalam contoh ini, karena Aturan B berlaku terakhir, nilai akhir `Severity` dalam temuan dari ID akun yang ditentukan adalah`INFORMATIONAL`. Berdasarkan tindakan Aturan A, nilai akhir `Confidence` dalam temuan yang cocok adalah`95`.

Third-party integrasi

Anda dapat menggunakan aturan otomatisasi untuk membuat tiket untuk integrasi dengan Jira Cloud danServiceNow ITSM. Untuk informasi selengkapnya, lihat Membuat aturan untuk integrasi pihak ketiga.

Skenario di mana aturan otomatisasi tidak berfungsi

Berikut ini adalah skenario di mana aturan otomatisasi tidak berfungsi.

- Akun mandiri menjadi anggota organisasi dengan admin yang didelegasikan
- Akun manajemen organisasi menghapus admin yang didelegasikan dan menetapkan admin baru yang didelegasikan
- Konfigurasi agregator untuk admin yang didelegasikan atau akun mandiri berubah ketika Wilayah yang tidak ditautkan dibuat Wilayah tertaut

Selama skenario ini, anggota organisasi dapat mengelola aturan otomatisasi dengan operasi daftar, dapatkan, dan hapus di API AWS CLI or.

Ketika Wilayah yang tidak ditautkan dibuat Wilayah tertaut, admin yang didelegasikan atau akun mandiri dapat mengelola sumber daya di Wilayah yang ditautkan dengan operasi daftar, dapatkan, dan hapus.

Membuat aturan otomatisasi di Hub Keamanan

Topik ini menjelaskan cara membuat aturan otomatisasi. Anda dapat menggunakan aturan otomatisasi untuk memperbarui detail untuk temuan atau membuat tiket untuk integrasi pihak ketiga. Anda harus membuat aturan otomatisasi secara individual dan di Wilayah AWS tempat yang Anda inginkan diterapkan. Namun, jika Anda membuat aturan otomatisasi di Wilayah agregasi, aturan tersebut diterapkan di semua Wilayah. Jika tidak, jika Anda membuat aturan otomatisasi di Wilayah yang tidak ditautkan, aturan tersebut hanya diterapkan di Wilayah tersebut.

Membuat aturan yang memperbarui rincian pencarian

Prosedur berikut menjelaskan cara membuat aturan yang memperbarui rincian pencarian.

1. Masuk ke AWS akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.

2. Dari panel navigasi, di bawah Manajemen, pilih Otomatisasi.
3. Pilih Buat aturan.
4. Di bawah Detail, masukkan nama untuk aturan otomatisasi Anda.
   - (Opsional) Masukkan deskripsi untuk aturan otomatisasi Anda.
5. Di bawah Tind akan, pilih Perbarui detail temuan. Anda dapat mencari kriteria dan menambahkan kriteria di bilah pencarian. Untuk memeriksa apakah ada temuan yang cocok dengan kriteria Anda, pilih Prat injau temuan yang cocok.
6. Di bawah Per barui detail pencarian, pilih setidaknya satu detail temuan untuk diperbarui saat temuan cocok dengan kriteria Anda. Anda dapat memilih tingkat keparahan, status, atau komentar.
7. Di bawah pengaturan aturan, pilih Di aktifkan atau Din onaktifkan. Jika Anda memilih Di aktifkan, aturan otomatisasi diaktifkan dan memproses temuan baru. Jika Anda memilih Din onaktifkan, aturan otomatisasi dinonaktifkan dan tidak memproses temuan apa pun.
8. (Opsional) Di bawah Tag, pilih Tambahkan tag baru untuk memasukkan pasangan kunci-nilai yang akan diterapkan pada aturan otomatisasi Anda.
9. Pilih Buat aturan.

Membuat aturan untuk integrasi pihak ketiga

Prosedur berikut menjelaskan cara membuat aturan yang membuat tiket untuk integrasi pihak ketiga. Untuk informasi tentang integrasi yang didukung Security Hub CSPM, lihat Third-party integrasi untuk Security Hub CSPM.

1. Masuk ke AWS akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, di bawah Manajemen, pilih Otomatisasi.
3. Pilih Buat aturan.
4. Di bawah Detail, masukkan nama untuk aturan otomatisasi Anda.
   - (Opsional) Masukkan deskripsi untuk aturan otomatisasi Anda.
5. Di bawah T indakan, pilih Buat tiket. Anda dapat mencari kriteria dan menambahkan kriteria di bilah pencarian. Untuk memeriksa apakah ada temuan yang cocok dengan kriteria Anda, pilih Prat injau temuan yang cocok.
6. Di bawah Buat tiket, pilih integrasi tiket TI dari dropdown, lalu pilih Tam bah integrasi.

7. Di bawah pengaturan aturan, pilih Di aktifkan atau Din onaktifkan. Jika Anda memilih Di aktifkan, aturan otomatisasi diaktifkan dan memproses temuan baru. Jika Anda memilih Din onaktifkan, aturan otomatisasi dinonaktifkan dan tidak memproses temuan apa pun.
8. (Opsional) Di bawah Tag, pilih Tambahkan tag baru untuk memasukkan pasangan kunci-nilai yang akan diterapkan pada aturan otomatisasi Anda.
9. Pilih Buat aturan.

Melihat detail untuk aturan otomatisasi di Hub Keamanan

Topik ini menjelaskan cara melihat detail untuk aturan otomatisasi. Anda dapat melihat detail berikut untuk aturan otomatisasi:

- Nama dan deskripsi
- Tindakan dan kriteria
- Status aturan dan temuan yang ada
- Tanda

Untuk melihat detail aturan otomatisasi

1. Masuk ke AWS akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, di bawah Manajemen, pilih Otomatisasi. Layar ini menampilkan semua aturan otomatisasi yang Anda buat.
3. Pilih aturan otomatisasi yang ingin Anda lihat. Pilih Lihat detail. Atau, Anda dapat memilih nama aturan otomatisasi yang ingin Anda lihat.

Memperbarui urutan aturan di Hub Keamanan

Topik ini menjelaskan cara memperbarui urutan aturan untuk aturan otomatisasi di konsol. Jika Anda ingin mengedit kriteria untuk aturan otomatisasi, lihat Meng edit aturan otomatisasi di Hub Keamanan.

Anda tidak dapat memperbarui urutan aturan untuk satu aturan otomatisasi tanpa memperbarui urutan aturan untuk setiap aturan otomatisasi. Misalnya, Anda memiliki empat aturan otomatisasi: Aturan A (1), Aturan B (2), Aturan C (3), dan Aturan D (4). Anda ingin Aturan D diterapkan terlebih

dahulu. Untuk melakukan ini, Anda mengubah nomornya dari 4 menjadi 1. Akibatnya, Aturan A mendapat 2, Aturan B mendapat 3, dan Aturan C mendapat 4.

Untuk memperbarui urutan aturan untuk aturan otomatisasi Anda

1. Masuk ke AWS akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, di bawah Manajemen, pilih Otomatisasi.
3. Pilih aturan otomatisasi yang ingin Anda edit. Di bawah Pesanan, pilih ikon pensil di sebelah nomor pesanan. Gunakan panah untuk menentukan nomor pesanan baru. Pilih ikon ✓ untuk mengonfirmasi. Pilih ikon X untuk membatalkan. Atau, Anda dapat memilih Ubah urutan untuk memindahkan aturan otomatisasi ke bawah, ke atas, atau ke bagian atas daftar.

Menonaktifkan aturan otomatisasi di Hub Keamanan

Topik ini menjelaskan cara menonaktifkan aturan otomatisasi. Saat Anda menonaktifkan aturan otomatisasi, Hub Keamanan berhenti menerapkannya. Anda dapat menonaktifkan aturan otomatisasi kapan saja dan di Wilayah AWS tempat Anda membuatnya.

Untuk menonaktifkan aturan

1. Masuk ke AWS akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, di bawah Manajemen, pilih Otomatisasi.
3. Pilih aturan otomatisasi yang ingin Anda nonaktifkan. Di bawah Status, pilih ikon pensil di samping Di aktifkan. Pilih dropdown, lalu pilih Din onaktifkan. Pilih ikon ✓ untuk mengonfirmasi. Pilih ikon X untuk membatalkan. Anda juga dapat memilih Non aktifkan dari menu tarik- turun T indakan.

Mengaktifkan aturan otomatisasi di Hub Keamanan

Topik ini menjelaskan cara mengaktifkan aturan otomatisasi. Saat Anda mengaktifkan aturan otomatisasi, Security Hub melanjutkan penerapannya. Anda dapat mengaktifkan aturan otomatisasi kapan saja dan di Wilayah AWS tempat Anda membuatnya.

Untuk mengaktifkan aturan

1. Masuk ke AWS akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, di bawah Manajemen, pilih Otomatisasi.
3. Pilih aturan otomatisasi yang ingin Anda aktifkan. Di bawah Status, pilih ikon pensil di sebelah Din onaktifkan. Pilih dropdown, lalu pilih Di aktifkan. Pilih ikon ✓ untuk mengonfirmasi. Pilih ikon X untuk membatalkan. Anda juga dapat memilih Aktifkan dari dropdown Tindakan.

Menduplikasi aturan otomatisasi di Hub Keamanan

Topik ini menjelaskan cara menduplikasi aturan otomatisasi. Menduplikasi aturan otomatisasi dapat membantu Anda menghemat waktu jika Anda ingin menghindari membuatnya dari awal. Saat menduplikasi aturan otomatisasi, Anda dapat memperbarui detail, tindakan, pengaturan aturan, dan tag. Anda dapat mengedit aturan otomatisasi Wilayah AWS di tempat Anda membuatnya.

Untuk menduplikasi aturan

1. Masuk ke AWS akun Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, dan pilih Otomatisasi.
3. Pilih aturan otomatisasi yang ingin Anda duplikat. Kemudian pilih T indakan, lalu pilih D uplikat.
4. Buat dan tinjau perubahan Anda, lalu pilih Buat aturan.

Mengedit aturan otomatisasi di Hub Keamanan

Topik ini menjelaskan cara mengedit aturan otomatisasi. Anda dapat mengedit aturan otomatisasi Wilayah AWS di tempat Anda membuatnya.

Anda dapat mengedit aturan otomatisasi berikut ini:

- Nama dan deskripsi
- Tindakan
- Pengaturan aturan

Anda tidak dapat mengedit tag untuk aturan otomatisasi.

Cara mengedit aturan

1. Masuk ke AWS akun Anda. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, di bawah Manajemen, pilih Otomatisasi.
3. Pilih aturan otomatisasi yang ingin Anda edit. Pilih Tindakan, dan kemudian pilih Edit.
4. Buat dan tinjau suntingan Anda.
5. Pilih Simpan perubahan.

Menghapus aturan otomatisasi di Hub Keamanan

Topik ini menjelaskan cara menghapus aturan otomatisasi. Anda dapat menghapus aturan otomatisasi Wilayah AWS di tempat Anda membuatnya.

Untuk menghapus aturan

1. Masuk ke AWS akun Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Otomatisasi.
3. Pilih aturan otomatisasi yang ingin Anda hapus. Pilih Tindakan, lalu pilih Hapus.
4. Pilih Hapus.

Aturan otomatisasi di EventBridge

Anda dapat menggunakan aturan otomatisasi di Amazon EventBridge untuk menanggapi temuan Security Hub. Security Hub mengirimkan temuan ke acara EventBridge as dalam waktu hampir real time. Anda dapat menulis aturan dasar yang menunjukkan tindakan otomatis apa yang harus diambil ketika suatu peristiwa cocok dengan aturan. Tindakan yang dapat dipicu secara otomatis meliputi:

- Mengkonfigurasi tujuan API di EventBridge.
- Memanggil perintah run Amazon EC2
- Menginvokasi fungsi Lambda
- Memanggil mesin status Fungsi Langkah
- Memberi tahu topik Amazon SNS atau antrean Amazon SQS
- Menyampaikan peristiwa ke Kinesis Data Streams

- Mengirim temuan ke alat manajemen tiket, obrolan, SIEM, atau respon insiden pihak ketiga
- Mengirim acara ke EventBridge bus di AWS akun lain

Security Hub mengirimkan temuan baru dan temuan terbaru ke acara EventBridge as. Kemudian Anda mengonfigurasi EventBridge aturan untuk merespons setiap peristiwa Hub Keamanan. Untuk informasi lebih lanjut, lihat Apa itu EventBridge? dalam Panduan EventBridge Pengguna.

> **Note**
>
> Jika Anda memiliki EventBridge aturan yang ditetapkan untuk temuan di Security Hub CSPM, aturan dapat tumpang tindih dengan aturan yang ditentukan untuk Hub Keamanan. Untuk menghindari pengiriman temuan duplikat, evaluasi aturan yang telah Anda tetapkan untuk Security Hub CSPM untuk menentukan apakah aturan tersebut tumpang tindih dengan aturan yang telah Anda tetapkan untuk Hub Keamanan. Jika berlaku, nonaktifkan aturan CSPM Security Hub yang diganti dengan aturan Hub Keamanan.

> **Note**
>
> Sebagai praktik terbaik, pastikan pengguna dengan izin untuk mengakses EventBridge menggunakan AWS Identity and Access Management kebijakan yang memberikan izin minimum yang diperlukan. Untuk informasi lebih lanjut, lihat EventBridge dan AWS Identity and Access Management di Panduan EventBridge Pengguna.

EventBridge jenis acara

Security Hub menggunakan jenis EventBridge acara Amazon berikut untuk diintegrasikan EventBridge.

Pada EventBridge dasbor untuk Hub Keamanan, Semua Acara menyertakan semua jenis acara ini.

Temuan yang Diimpor V2

Security Hub secara otomatis mengirimkan semua temuan baru dan semua pembaruan untuk temuan yang ada ke Findings Imported V2 acara EventBridge as. Setiap Findings Imported V2 peristiwa berisi satu temuan.

Setiap temuan yang diimpor dan setiap temuan yang diperbarui melalui `BatchUpdateFindingsV2` permintaan memicu Findings Imported V2 peristiwa.

Untuk akun administrator, umpan acara menyer EventBridge takan peristiwa untuk temuan dari akun mereka dan dari akun anggota mereka.

Di Wilayah agregasi, umpan peristiwa menyertakan peristiwa untuk temuan dari Wilayah agregasi dan Wilayah yang ditautkan. Cross-Region temuan disertakan dalam umpan acara hampir secara real time.

Anda dapat menentukan aturan EventBridge yang secara otomatis merutekan temuan ke alur kerja remediasi, alat pihak ketiga, atau EventBridge target https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-targets.html lain yang didukung. Aturan dapat menyertakan filter yang hanya menerapkan aturan jika temuan memiliki nilai atribut tertentu.

Anda menggunakan metode ini untuk secara otomatis mengirim semua temuan, atau semua temuan yang memiliki karakteristik tertentu, ke alur kerja respons atau remediasi.

> **Note**
>
> Security Hub dan Security Hub CSPM keduanya mengirim temuan ke EventBridge bawah sumber. `aws.securityhub` Pastikan EventBridge aturan Anda menggunakan tipe detail khusus untuk Security Hub untuk menghindari duplikat pemberitahuan terkait dengan temuan CSPM Security Hub.

EventBridge format acara

Jenis Findings Imported V2 acara menggunakan format acara berikut.

Contoh

Format ini digunakan saat Hub Keamanan mengirim acara ke EventBridge.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Findings Imported V2",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
```

```
   "region":"us-west-2",
   "resources":[
      "e51603d1054aad9d9f498d82d6e81acf4cf6bc88140e8ad2273123c73b81084"
   ],
   "detail":{
      "findings": [{
         <finding content>
       }]
   }
}
```

Setiap peristiwa mengirimkan satu temuan. *<finding content>*adalah konten dalam JSON dari temuan yang dikirim oleh acara tersebut.

Untuk daftar lengkap atribut pencarian, lihat temuan OCSF di Security Hub C SPM.

Mengkonfigurasi aturan untuk EventBridge

Anda dapat membuat aturan di Amazon EventBridge yang menentukan tindakan yang harus diambil saat Findings Imported V2 acara diterima. Findings Imported V2peristiwa dipicu oleh pembaruan melalui `BatchUpdateFindingsV2`.

Setiap aturan berisi pola peristiwa, yang mengidentifikasi peristiwa yang memicu aturan. Pola acara selalu berisi sumber peristiwa (`aws.securityhub`) dan jenis peristiwa (Findings Imported V2). Pola peristiwa juga dapat menentukan filter untuk mengidentifikasi temuan yang berlaku aturan.

Aturan acara kemudian mengidentifikasi target aturan. Target adalah tindakan yang harus diambil saat EventBridge menerima peristiwa F indings Im ported V2 dan temuan cocok dengan filter.

Instruksi yang diberikan di sini menggunakan EventBridge konsol. Saat Anda menggunakan konsol, EventBridge secara otomatis membuat kebijakan berbasis sumber daya yang diperlukan yang memungkinkan EventBridge untuk menulis ke Amazon CloudWatch Log.

Anda juga dapat menggunakan `PutRule` operasi EventBridge API. Namun, jika Anda menggunakan EventBridge API, maka Anda harus membuat kebijakan berbasis sumber daya. Untuk informasi tentang kebijakan yang diperlukan, lihat CloudWatch Iz in log di Panduan EventBridge Pengguna Amazon.

Format pola acara

Format pola acara untuk peristiwa Find ings Imported V2 adalah sebagai berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`mengidentifikasi Hub Keamanan sebagai layanan yang menghasilkan acara.
- `detail-type`mengidentifikasi jenis peristiwa.
- `detail`bersifat opsional dan menyediakan nilai filter untuk pola acara. Jika pola peristiwa tidak berisi `detail` bidang, maka semua temuan memicu aturan.

Anda dapat memfilter temuan berdasarkan atribut pencarian apa pun. Untuk setiap atribut, Anda menyediakan array yang dipisahkan koma dari satu atau lebih nilai.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Jika Anda memberikan lebih dari satu nilai untuk atribut, maka nilai-nilai tersebut digabungkan dengan`OR`. Penemuan cocok dengan filter untuk atribut individual jika temuan memiliki salah satu nilai yang tercantum. Misalnya, jika Anda memberikan keduanya `INFORMATIONAL` dan `LOW` sebagai nilai untuk`Severity.Label`, maka temuan cocok jika memiliki label keparahan salah satu `INFORMATIONAL` atau`LOW`.

Atribut bergabung dengan`AND`. Penemuan cocok jika cocok dengan kriteria filter untuk semua atribut yang disediakan.

Saat Anda memberikan nilai atribut, nilai tersebut harus mencerminkan lokasi atribut tersebut dalam struktur AWS Open Cybersecurity Schema Framework (OCSF).

Dalam contoh berikut, pola peristiwa memberikan nilai filter untuk `ProductArn` dan`Severity.Label`, jadi temuan cocok jika dibuat oleh Amazon Inspector dan memiliki label keparahan salah satu `INFORMATIONAL` atau`LOW`.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Findings Imported V2"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Membuat aturan acara

Anda dapat menggunakan pola peristiwa yang telah ditentukan atau pola peristiwa khusus untuk membuat aturan di EventBridge. Jika Anda memilih pola yang telah ditentukan, EventBridge secara otomatis mengisi `source` dan`detail-type`. EventBridge juga menyediakan bidang untuk menentukan nilai filter untuk atribut pencarian berikut:

- `cloud.account.uid`
- `compliance.status`
- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

Untuk membuat EventBridge aturan (konsol)

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Menggunakan nilai-nilai berikut, buat EventBridge aturan yang memantau peristiwa pencarian:
    - Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
    - Pilih cara membangun pola acara.

Untuk membangun pola acara dengan...	Lakukan ini...	
Sebuah templat	Di bagian Pola acara, pilih opsi berikut: • Untuk Sumber peristiwa, pilih Layanan AWS . • Untuk AWS layanan, pilih Hub Keamanan. • Untuk Jenis acara, pilih Find ings Imported V2. • (Opsional) Untuk membuat aturan lebih spesifik, tambahkan nilai filter. Misalnya, untuk membatasi aturan pada temuan dengan status rekaman aktif, untuk status Rekaman Khusus, pilih Aktif.	

Untuk membangun pola acara dengan...	Lakukan ini...
Pola acara khusus (Gunakan pola khusus jika Anda ingin memfilter temuan berdasarkan atribut yang tidak muncul di EventBridge konsol.)	• Di bagian Pola acara, pilih Pola khusus (editor JSON), lalu tempel pola peristiwa berikut ke area teks: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Findings Imported V2" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>"] } } }` • Perbarui pola peristiwa untuk menyertakan nilai atribut dan atribut yang ingin Anda gunakan sebagai filter. Misalnya, untuk menerapkan aturan pada temuan yang memiliki tingkat keparahan `Critical`, gunakan contoh pola berikut:

Untuk membangun pola acara dengan...	Lakukan ini...	

	<pre>{
	"source":
	["aws.securityhub"
	],
	"detail-type":
	["Findings Imported
	V2"],
	"detail":{
	"findings":
	{
	"Severity
	": ["Critical"]
	}
	}
	}</pre>	

- Untuk Jenis Target, pilih AWS layanan, dan untuk Pilih target, pilih target seperti topik atau AWS Lambda fungsi Amazon SNS. Target terpicu saat peristiwa diterima yang sesuai dengan pola peristiwa yang ditentukan dalam aturan.

Untuk detail tentang membuat aturan, lihat Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa di Panduan EventBridge Pengguna Amazon.

> **Note**
>
> Jika Anda memiliki EventBridge aturan yang ditetapkan untuk temuan di Security Hub CSPM, aturan dapat tumpang tindih dengan aturan yang ditentukan untuk Hub Keamanan. Untuk menghindari pengiriman temuan duplikat, evaluasi aturan yang telah Anda tetapkan untuk Security Hub CSPM untuk menentukan apakah aturan tersebut tumpang tindih dengan aturan yang telah Anda tetapkan untuk Hub Keamanan. Jika berlaku, nonaktifkan aturan CSPM Security Hub yang diganti dengan aturan Hub Keamanan.

Third-party integrasi untuk Security Hub

Anda dapat meningkatkan postur keamanan Anda dengan integrasi pihak ketiga untuk Hub AWS Keamanan. Dengan fitur ini, Anda dapat mengaktifkan integrasi yang menggunakan temuan dari Security Hub, memungkinkan Anda untuk menggabungkan alat operasional, investigasi, dan respons Anda dengan Security Hub. Saat ini Security Hub mendukung integrasi dengan Jira Cloud danServiceNow.

Topik

- Integrasi untuk AWS Hub Keamanan Jira Cloud
- Integrasi untuk ServiceNow
- Kebijakan kunci KMS untuk integrasi tiket Security Hub
- Menguji integrasi tiket yang dikonfigurasi

Integrasi untuk AWS Hub Keamanan Jira Cloud

Topik ini menjelaskan cara mengintegrasikan Hub Keamanan denganJira Cloud. Sebelum menyelesaikan salah satu prosedur dalam topik ini, Anda harus membeli paket Jira Cloud berlangganan. Untuk informasi tentang paket berlangganan, lihat Harga di Atlassian situs web.

Integrasi ini memungkinkan Anda mengirim temuan Security Hub ke Jira Cloud, secara manual atau otomatis, sehingga Anda dapat mengelolanya sebagai bagian dari alur kerja operasional Anda. Misalnya, Anda dapat menetapkan kepemilikan untuk masalah yang memerlukan penyelidikan dan remediasi.

Untuk akun dalam organisasi, hanya administrator yang didelegasikan yang dapat mengonfigurasi integrasi. Administrator yang didelegasikan dapat menggunakan fitur buat tiket secara manual untuk setiap temuan akun anggota. Selain itu, administrator yang didelegasikan dapat menggunakan aturan otomatisasi untuk secara otomatis membuat tiket untuk temuan apa pun yang terkait dengan akun anggota. Saat menentukan aturan otomatisasi, administrator yang didelegasikan dapat menetapkan kriteria, yang dapat mencakup semua akun anggota atau akun anggota tertentu. Untuk informasi tentang menyetel administrator yang didelegasikan, lihat Mengatur akun administrator yang didelegasikan di Hub Keamanan.

Untuk akun yang tidak berada di organisasi, semua aspek fitur ini tersedia.

Prasyarat

Sebelum menghubungkan Hub Keamanan dengan Jira Cloud lingkungan Anda, Anda harus memastikan bahwa langkah-langkah konfigurasi berikut dilakukan di lingkungan Jira Anda.

- Instal Hub AWS Keamanan untuk aplikasi cloud Jira.
- Memiliki setidaknya satu proyek pengembangan perangkat lunak yang dikelola perusahaan.
- Tetapkan AWS aplikasi ke proyek pengembangan perangkat lunak yang ingin Anda terima temuan dari Security Hub.

Langkah-langkah untuk masing-masing prasyarat ini tercantum di bawah ini.

1. Instal AWS Hub Keamanan untuk Jira Cloud aplikasi

Security Hub memiliki aplikasi untuk mendukung integrasinya dengan Jira. Aplikasi ini menginstal bidang khusus dan jenis masalah khusus. Security Hub menggunakan ini untuk mengisi atribut tertentu tentang temuan.

1. Masuk ke Atlassian situs Anda sebagai administrator.
2. Pilih Pengaturan, dan pilih Aplikasi.
3. Jika diarahkan ke halaman pasar, pilih Cari aplikasi baru. Jika diarahkan ke halaman aplikasi, pilih Jelaj ahi aplikasi, lalu cari Hub AWS Keamanan untuk Jira Cloud. Kemudian pilih Dapatkan sekarang.

2. Membuat proyek atau memverifikasi proyek yang ada

Langkah ini diperlukan jika Anda belum membuat proyek. Untuk informasi tentang cara membuat proyek, lihat Membuat proyek baru dalam Jira Cloud Support dokumentasi.

Persyaratan untuk membuat proyek

Pastikan untuk melakukan hal berikut saat membuat proyek baru.

- Pilih Pengembangan perangkat lunak untuk template proyek.
- Pilih Company-managed untuk jenis proyek.

Persyaratan untuk proyek yang ada

Setiap proyek yang ada di lingkungan Jira Anda yang terintegrasi dengan Security Hub harus merupakan jenis Company-managed proyek.

3. Tambahkan proyek Anda ke AWS Hub Keamanan untuk Jira Cloud aplikasi

Agar Hub Keamanan dapat berhasil mengirim temuan ke lingkungan Jira Anda, setiap proyek yang ingin Anda gunakan dengan Hub Keamanan harus dikaitkan dengan Hub AWS Keamanan untuk Jira Cloud aplikasi. Mengaitkan proyek Jira dengan aplikasi memastikan bahwa bidang kustom yang diperlukan untuk Hub Keamanan dikaitkan dengan proyek dan dapat diisi saat Hub Keamanan mengirimkan temuan ke proyek.

1. Masuk ke Atlassian situs Anda sebagai administrator.
2. Pilih Pengaturan, dan pilih Aplikasi.
3. Dari daftar aplikasi, pilih Hub AWS Keamanan untuk Jira Cloud.
4. Pilih tab Pengaturan konektor.
5. Di bawah Proyek diaktifkan, pilih Tambahkan Proyek Jira.
    a. Dari dropdown, pilih Tambahkan semua, atau pilih proyek. Ulangi bagian langkah ini jika Anda ingin menambahkan lebih dari satu proyek, tetapi tidak semua proyek.
    b. Pilih Simpan.

Anda dapat memverifikasi proyek mana yang telah berhasil diinstal dari tab Manajer Instalasi. Anda juga dapat memverifikasi konfigurasi untuk bidang, layar, status, dan alur kerja dari tab Manajer Instalasi.

Untuk informasi tambahan mengenaiJira Cloud, lihat Jira Cloud sumber daya di Atlassian situs web.

Rekomendasi

Membuat akun sistem khusus untuk lingkungan Jira Anda

Integrasi Hub Keamanan Jira Cloud menggunakan koneksi OAuth yang terkait dengan pengguna tertentu dalam instans Jira Anda. Membuat akun sistem khusus untuk digunakan untuk koneksi OAuth Hub Keamanan Anda disarankan untuk koneksi Anda karena alasan berikut:

- Pengguna sistem khusus memastikan bahwa koneksi tidak terkait dengan karyawan yang izin ke lingkungan Jira dapat berubah seiring waktu, berdampak pada kemampuan Hub Keamanan untuk berintegrasi dengan lingkungan Jira Anda.

- Setiap masalah yang dibuat Hub Keamanan di Jira menampilkan bidang Created By yang berisi nama pengguna yang digunakan untuk membuat koneksi OAuth. Menggunakan akun sistem untuk koneksi OAuth menghasilkan akun sistem ini muncul sebagai pembuat tiket, membantu memberikan visibilitas bahwa temuan dibuat melalui integrasi Hub Keamanan dan bukan secara manual oleh pengguna Jira lain.

Konfigurasikan integrasi antara Hub Keamanan dan Jira Cloud

Prosedur berikut harus diselesaikan untuk setiap Jira Cloud proyek yang ingin Anda kirimi temuan Hub Keamanan.

> **Note**
>
> Saat Anda membuat Jira Cloud konektor, Anda dialihkan dari saat ini Wilayah AWS ke`"https://3rdp.oauth.console.api.aws"`, sehingga Anda dapat menyelesaikan pendaftaran konektor. Setelah itu, Anda dikembalikan ke Wilayah AWS tempat konektor sedang dibuat.

Untuk mengkonfigurasi integrasi untuk Jira Cloud

1. Masuk ke AWS akun Anda dengan kredenSIAL Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home? wilayah = us-east-1.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Integrasi.
3. Pilih TambahkanJira Cloud.
4. Untuk Detail, masukkan nama unik dan deskriptif untuk integrasi Anda, dan tentukan apakah akan memasukkan deskripsi opsional untuk integrasi Anda.
5. Untuk Enkripsi pilih cara Anda ingin mengenkripsi kredenSIAL integrasi Anda dalam Security Hub.

    - Gunakan kunci yang AWS dimiliki - Dengan opsi ini, kunci layanan milik Security Hub digunakan untuk mengenkripsi data kredensi integrasi Anda dalam Security Hub.
    - Pilih kunci KMS yang berbeda (lanjutan) - Dengan opsi ini Anda memilih AWS KMS key yang telah Anda buat yang ingin Anda gunakan untuk mengenkripsi data kredensi integrasi Anda dalam Security Hub. Untuk informasi tentang cara membuat AWS KMS kunci, lihat Membuat AWS KMS kunci di Panduan Peng AWS Key Management Service embang. Jika Anda memilih untuk menggunakan kunci Anda sendiri, Anda harus menambahkan pernyataan

kebijakan ke kunci KMS yang memungkinkan akses Hub Keamanan ke kunci tersebut. Lihat kebijakan AWS KMS utama untuk integrasi tiket Security Hub untuk detail tentang kebijakan yang diperlukan.

> **Note**
>
> Anda tidak dapat mengubah pengaturan ini setelah Anda menyelesaikan konfigurasi ini. Namun, Jika Anda memilih K unci yang disesuaikan, Anda dapat mengedit kebijakan kunci yang disesuaikan kapan saja.

6. (Opsional) Untuk Tag, buat dan tambahkan tag ke integrasi Anda. Anda dapat menambahkan hingga 50 tag.
7. Untuk O torisasi, pilih Buat konektor dan otorisasi. Muncul pop-up di mana Anda memilih Izinkan untuk menyelesaikan otorisasi. Setelah Anda menyelesaikan otorisasi, kotak centang muncul yang memberi tahu Anda bahwa otorisasi berhasil.
8. Untuk Konfigur asi, masukkan ID Jira Cloud proyek.
9. Pilih Konfigur asi lengkap. Setelah menyelesaikan konfigurasi, Anda dapat melihat integrasi yang dikonfigurasi di tab Integrasi yang dikonfigurasi.

Setelah mengkonfigurasi integrasi dengan Jira, Anda dapat menguji koneksi untuk mengonfirmasi bahwa semuanya dikonfigurasi dengan benar di lingkungan Jira Anda dan di Hub Keamanan. Untuk informasi selengkapnya, lihat Meng uji integrasi tiket yang dikonfigurasi.

Detail integrasi Jira tambahan

Pertimbangan batas tarif

Jira memberlakukan batas tarif API untuk menjaga stabilitas layanan dan memastikan penggunaan wajar di seluruh platform mereka. Saat menggunakan integrasi Hub AWS Keamanan dengan Jira, batas tarif ini dapat memengaruhi pemrosesan temuan Security Hub, terutama di lingkungan yang menghasilkan volume temuan yang tinggi. Hal ini dapat mengakibatkan pembuatan tiket tertunda, dan dalam skenario dengan volume temuan yang sangat tinggi, beberapa temuan mungkin tidak diproses menjadi tiket Jira sama sekali. Untuk mengoptimalkan integrasi Anda, pertimbangkan untuk menerapkan filter pada aturan Otomasi di Hub Keamanan untuk memprioritaskan ticketing pada temuan paling penting, memantau penggunaan Jira API Anda melalui konsol admin mereka, dan merencanakan alur kerja Anda berdasarkan batas tarif spesifik tingkat lisensi Jira Anda. Untuk implementasi bisnis penting, hubungi administrator Jira Anda untuk meninjau alokasi batas tarif Anda.

Untuk informasi terperinci tentang batas tarif Jira API, lihat dokumentasi pembatasan tarif di situs web Panduan Pengembang Atlassian.

Otentikasi dan keamanan

Otentikasi Jira API memerlukan konfigurasi OAuth 2.0 yang tepat untuk akses aman. Pastikan aplikasi Anda mengikuti praktik terbaik keamanan Atlassian untuk integrasi API.

Sumber Daya:

- Jira REST API v3: Dokumentasi Jira REST API v3 di situs web Atlassian
- Menerapkan OAuth 2.0 (3LO): Panduan implementasi OAuth 2.0 (3LO) di situs web Atlassian
- Mengelola aplikasi Jira Cloud: Sumber daya administrasi Jira Cloud di situs web Atlassian
- Kelola izin Jira: Kel ola izin proyek di situs web Atlassian

Membuat tiket untuk Jira Cloud integrasi

Setelah Anda membuat integrasi denganJira Cloud, Anda dapat membuat tiket untuk temuan.

> **Note**
>
> Penemuan akan selalu dikaitkan dengan satu tiket melalui seluruh siklus hidupnya. Security Hub mengirimkan semua pembaruan berikutnya ke temuan ke tiket yang sama setelah pembuatan awal. Jika konektor yang terkait dengan aturan otomatisasi diubah, konektor yang diperbarui hanya digunakan untuk temuan baru dan masuk yang sesuai dengan kriteria aturan.

Untuk membuat tiket untuk temuan

1. Masuk ke AWS akun Anda dengan kredensional Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home? wilayah = us-east-1.
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan. Dalam temuan, pilih Buat tiket.
4. Untuk Integr asi, buka menu dropdown, dan pilih integrasi. Integrasi ini adalah integrasi yang Anda buat sebelumnya ketika Anda mengonfigurasi Jira Cloud proyek. Pilih integrasi tempat Anda ingin temuan dikirim.
5. Pilih Buat.

Melihat tiket untuk a Jira Cloud integrasi

Setelah Anda membuat tiket untuk temuan, Anda dapat membuka tiket pada Jira Cloud instance Anda.

Untuk melihat temuan pada Anda Jira Cloud instans

1. Masuk ke AWS akun Anda dengan kredensional Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home? wilayah = us-east-1.
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan tempat Anda membuat tiket.
4. Dalam temuan, pilih ID tiket untuk melihat tiket pada Jira Cloud instance Anda atau Lihat JSON.

Integrasi untuk ServiceNow

Topik ini menjelaskan cara mengakses konsol Hub Keamanan untuk mengonfigurasi integrasiServiceNow ITSM. Sebelum menyelesaikan salah satu prosedur dalam topik ini, Anda harus berlangganan ServiceNow ITSM sebelum Anda dapat menambahkan integrasi ini. Untuk informasi lebih lanjut, lihat halaman harga di ServiceNow situs web.

Untuk akun dalam organisasi, hanya administrator yang didelegasikan yang dapat mengonfigurasi integrasi. Administrator yang didelegasikan dapat menggunakan fitur buat tiket secara manual untuk setiap temuan akun anggota. Selain itu, administrator yang didelegasikan dapat menggunakan aturan otomatisasi untuk secara otomatis membuat tiket untuk temuan apa pun yang terkait dengan akun anggota. Saat menentukan aturan otomatisasi, administrator yang didelegasikan dapat menetapkan kriteria, yang dapat mencakup semua akun anggota atau akun anggota tertentu. Untuk informasi tentang menyetel administrator yang didelegasikan, lihat Mengatur akun administrator yang didelegasikan di Hub Keamanan.

Untuk akun yang tidak berada di organisasi, semua aspek fitur ini tersedia.

Prasyarat - konfigurasikan ServiceNow lingkungan

Anda harus menyelesaikan prasyarat berikut sebelum mengonfigurasi integrasi untukServiceNow ITSM. Jika tidak, integrasi Anda antara ServiceNow ITSM dan Hub Keamanan tidak berfungsi.

1. Instal integrasi Security Hubfinding untuk Manajemen Layanan TI (ITSM)

Prosedur berikut menjelaskan cara menginstal plugin Security Hub.

1. Masuk ke ServiceNow ITSM instance Anda, lalu buka navigator aplikasi.
2. Arahkan ke ServiceNow Toko.
3. Cari integrasi temuan Hub Keamanan untuk Manajemen Layanan TI (ITSM), lalu pilih Dapatkan untuk menginstal aplikasi.

> **Note**
>
> Dalam pengaturan untuk aplikasi Hub Keamanan, pilih tindakan yang akan diambil saat temuan Hub Keamanan baru dikirim ke ServiceNow ITSM lingkungan Anda. Anda dapat memilih Jangan lakukan apa-apa, Buat insiden, Buat masalah, atau Buat keduanya (incident/problem).

2. Konfigurasikan jenis pemberian KredenSIAL Klien untuk permintaan OAuth masuk

Anda harus mengonfigurasi jenis hibah ini untuk permintaan OAuth masuk. Untuk informasi selengkapnya, lihat Jenis hibah Kredensi Klien untuk OAuth Masuk didukung di halaman web Dukungan. ServiceNow

3. Buat aplikasi OAuth

Jika Anda sudah membuat aplikasi OAuth, Anda dapat melewati prasyarat ini. Untuk informasi tentang membuat aplikasi OAuth, lihat Men yiapkan OAuth di situs web. ServiceNow

Prasyarat - konfigurasikan AWS Secrets Manager

Untuk menggunakan integrasi Security Hub ServiceNow, kredenSIAL untuk aplikasi ServiceNow OAuth Anda harus disimpan di Secrets Manager. Menyimpan kredenSIAL Anda di Secrets Manager memungkinkan Anda memiliki kontrol dan visibilitas ke dalam penggunaan kredenSIAL sementara juga mengizinkan Security Hub menggunakan kredenSIAL untuk diintegrasikan dengan ServiceNow instans Anda. Untuk menyimpan kredenSIAL Anda di Secrets Manager, Anda harus menggunakan AWS KMS kunci yang dikelola pelanggan untuk melindungi rahasia. K AWS KMS unci ini memungkinkan Anda untuk melindungi rahasia saat disimpan saat istirahat dan juga memungkinkan kebijakan dilampirkan ke kunci yang memberikan izin Hub Keamanan untuk mengakses kunci yang melindungi rahasia.

Gunakan langkah-langkah berikut untuk mengonfigurasi Manajer Rahasia untuk ServiceNow kredenSIAL Anda.

Langkah 1: Lampirkan kebijakan ke AWS KMS kunci

Agar berhasil mengkonfigurasi ServiceNow integrasi Anda, Anda harus terlebih dahulu memberikan izin Security Hub untuk menggunakan AWS KMS kunci yang terkait dengan ServiceNow kredenSIAL Anda di Secrets Manager.

Untuk memodifikasi AWS KMS kebijakan kunci untuk Security Hub untuk mengakses ServiceNow kredensibilitas Anda

1. Buka AWS KMS konsol di https://console.aws.amazon.com/kms.
2. Untuk mengubah Wil AWS ayah, gunakan pemilih Wilayah di sudut kanan atas halaman.
3. Pilih AWS KMS kunci yang ada atau lakukan langkah-langkah untuk Membuat kunci baru di Panduan Peng AWS KMS embang.
4. Di bagian Kebijakan utama, pilih Edit.
5. Jika Tampilan Beralih ke kebijakan ditampilkan, pilih untuk menampilkan kebijakan Kunci, lalu pilih Edit.
6. Salin blok kebijakan berikut ke kebijakan AWS KMS kunci Anda, untuk memberikan izin Hub Keamanan untuk menggunakan kunci Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Sid": "Enable IAM User Permissions",
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::your-account-id:root"
        },
        "Action": "kms:*",
        "Resource": "*"
        },
        {
        "Sid": "Allow Security Hub connector service to decrypt secrets",
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "kms:Decrypt",
        "Resource": "*",
        "Condition": {
```

```
            "StringEquals": {
            "kms:ViaService": "secretsmanager.your-region.amazonaws.com"
            },
            "StringLike": {
            "kms:EncryptionContext:SecretARN": "arn:aws:secretsmanager:your-
region:your-account-id:secret:ServiceNow*"
            }
        }
        }
    ]
    }
```

7. Edit kebijakan dengan mengganti nilai-nilai berikut dalam contoh kebijakan:
   - Ganti *your-account-id* dengan ID AWS akun Anda.
   - Ganti *your-region* dengan AWS wilayah Anda (misalnya,`us-east-1`).
8. Jika Anda menambahkan pernyataan kebijakan sebelum pernyataan akhir, tambahkan koma sebelum menambahkan pernyataan ini. Pastikan sintaks JSON kebijakan AWS KMS kunci Anda valid.
9. Pilih Simpan.
10. (Opsional) Salin kunci ARN ke notepad untuk digunakan pada langkah selanjutnya.

Langkah 2: Buat rahasia di Manajer Rahasia

Buat rahasia di Secrets Manager yang akan menyimpan ServiceNow kredensibilitas Anda. Security Hub akan mengakses rahasia ini saat berinteraksi dengan ServiceNow lingkungan Anda.

Ikuti langkah-langkah Untuk membuat rahasia di Panduan AWS Secrets Manager Pengguna. Setelah Anda membuat rahasia Anda, salin ARN Rahasia karena Anda akan membutuhkannya saat membuat konektor Hub Keamanan Anda.

Saat membuat rahasia, pastikan Anda mengonfigurasi yang berikut:

Jenis rahasia

Jenis rahasia lainnya

Key/value pasangan (format Plainteks)

```
{
    "ClientId": "your-servicenow-client-id",
```

```
    "ClientSecret": "your-servicenow-client-secret"
    }
```

> **Note**
>
> Nama bidang harus persis `ClientId` dan `ClientSecret` (peka huruf besar). Security Hub memerlukan nama-nama yang tepat ini untuk mengambil kredenSIAL.

Kunci enkripsi

Gunakan AWS KMS kunci yang Anda konfigurasikan pada Langkah 1

Kebijakan sumber daya

Gunakan kebijakan sumber daya berikut:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Principal": {
            "Service": "connector.securityhub.amazonaws.com"
        },
        "Action": "secretsmanager:GetSecretValue",
        "Resource": "arn:aws:secretsmanager:your-region:your-account-
id:secret:ServiceNow*",
        "Condition": {
            "StringEquals": {
            "aws:SourceAccount": "your-account-id",
            "aws:SourceArn": "arn:aws:securityhub:your-region:your-account-id:*"
            }
        }
        }
    ]
    }
```

Sekarang rahasia Anda dikonfigurasi, Anda dapat membuat konektor Hub Keamanan menggunakan API atau AWS Konsol CreateConnector V2. Anda harus menyediakan:

- InstanceName: URL ServiceNow instans Anda (misalnya,`your-instance.service-now.com`)

- SecretArn: ARN rahasia yang Anda buat dalam prosedur ini

Konfigurasikan integrasi untuk ServiceNow ITSM

Security Hub dapat membuat insiden atau masalah secara otomatisServiceNow ITSM.

Untuk mengkonfigurasi integrasi untuk ServiceNow ITSM

1. Masuk ke AWS akun Anda dengan kredenSIAL Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home? wilayah = us-east-1.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Integrasi.
3. Di bawah ServiceNow ITSM, pilih Tambahkan integrasi.
4. Untuk Detail, masukkan nama untuk integrasi Anda, dan tentukan apakah akan memasukkan deskripsi opsional untuk integrasi Anda.
5. Untuk Enkripsi pilih cara Anda ingin mengenkripsi kredenSIAL integrasi Anda dalam Security Hub.

   - Gunakan kunci yang AWS dimiliki - Dengan opsi ini, kunci layanan milik Security Hub digunakan untuk mengenkripsi data kredensi integrasi Anda dalam Security Hub.
   - Pilih kunci KMS yang berbeda (lanjutan) - Dengan opsi ini Anda memilih AWS KMS key yang telah Anda buat yang ingin Anda gunakan untuk mengenkripsi data kredensi integrasi Anda dalam Security Hub. Untuk informasi tentang cara membuat AWS KMS kunci, lihat Membuat AWS KMS kunci di Panduan Peng AWS Key Management Service embang. Jika Anda memilih untuk menggunakan kunci Anda sendiri, Anda harus menambahkan pernyataan kebijakan ke kunci KMS yang memungkinkan akses Hub Keamanan ke kunci tersebut. Lihat kebijakan AWS KMS utama untuk integrasi tiket Security Hub untuk detail tentang kebijakan yang diperlukan.

   > **Note**
   >
   > Anda tidak dapat mengubah pengaturan ini setelah Anda menyelesaikan konfigurasi ini. Namun, Jika Anda memilih K unci yang disesuaikan, Anda dapat mengedit kebijakan kunci yang disesuaikan kapan saja.

6. Untuk Kredensi, masukkan ServiceNow ITSM URL Anda, dan ARN AWS Secrets Manager rahasia Anda yang dibuat di bagian prasyarat.

7. Untuk Tag, tentukan apakah akan membuat dan menambahkan tag opsional ke integrasi Anda.
8. Pilih Tambahkan integrasi. Setelah menyelesaikan konfigurasi, Anda dapat melihat integrasi yang dikonfigurasi di tab Integrasi yang dikonfigurasi.

Setelah mengonfigurasi integrasi dengan ServiceNow, Anda dapat menguji koneksi untuk mengonfirmasi bahwa semuanya dikonfigurasi dengan benar di ServiceNow lingkungan Anda dan di Hub Keamanan. Untuk informasi selengkapnya, lihat Meng uji integrasi tiket yang dikonfigurasi.

Membuat tiket untuk ServiceNow ITSM integrasi

Setelah Anda membuat integrasi denganServiceNow ITSM, Anda dapat membuat tiket untuk temuan.

> **Note**
>
> Penemuan akan selalu dikaitkan dengan satu tiket melalui seluruh siklus hidupnya. Security Hub mengirimkan semua pembaruan berikutnya ke temuan ke tiket yang sama setelah pembuatan awal. Jika konektor yang terkait dengan aturan otomatisasi diubah, konektor yang diperbarui hanya digunakan untuk temuan baru dan masuk yang sesuai dengan kriteria aturan.

Untuk membuat tiket untuk temuan

1. Masuk ke AWS akun Anda dengan kredensional Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home? wilayah = us-east-1.
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan. Dalam temuan, pilih Buat tiket.
4. Untuk Integr asi, buka menu dropdown, dan pilih integrasi.
5. Pilih Buat.

Melihat tiket untuk ServiceNow ITSM integrasi

Setelah Anda membuat tiket untuk temuan, Anda dapat membuka tiket pada ServiceNow ITSM instance Anda.

Untuk melihat temuan pada Anda ServiceNow ITSM instans

1. Masuk ke AWS akun Anda dengan kredensibilitas Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home? wilayah = us-east-1.
2. Dari panel navigasi, di bawah Inventaris, pilih Temuan.
3. Pilih temuan tempat Anda membuat tiket.
4. Dalam temuan, pilih ID tiket untuk melihat tiket pada ServiceNow ITSM instance Anda atau Lihat JSON.

Kebijakan kunci KMS untuk integrasi tiket Security Hub

Saat menggunakan kunci KMS yang dikelola pelanggan dengan integrasi tiket Security Hub, kebijakan tambahan perlu ditambahkan ke kunci KMS agar Security Hub dapat berinteraksi dengan kunci tersebut. Selain itu, kebijakan perlu ditambahkan yang memungkinkan kepala sekolah yang menambahkan kunci ke izin konektor Hub Keamanan untuk mengakses kunci.

Kebijakan izin Hub Keamanan

Kebijakan berikut menguraikan izin yang diperlukan Hub Keamanan untuk dapat mengakses dan menggunakan kunci KMS yang terkait dengan Jira dan ServiceNow konektor Anda. Kebijakan ini perlu ditambahkan ke setiap kunci KMS yang terkait dengan konektor Hub Keamanan.

Kebijakan ini berisi izin berikut:

- Memungkinkan Security Hub untuk melindungi, mengakses sementara, atau menyegarkan token yang digunakan untuk berkomunikasi dengan integrasi tiket Anda, menggunakan kunci. Izin dibatasi untuk operasi yang terkait dengan konektor Hub Keamanan tertentu melalui blok kondisi yang memeriksa ARN sumber dan konteks enkripsi.
- Memungkinkan Security Hub untuk membaca metadata tentang kunci KMS dengan mengizinkan `DescribeKey` operasi. Izin ini diperlukan untuk Security Hub untuk memverifikasi status dan konfigurasi kunci. Akses terbatas pada konektor Hub Keamanan tertentu melalui kondisi ARN sumber.

```
{
    "Sid": "Allow Security Hub access to the customer managed key",
    "Effect": "Allow",
```

```
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:connectorV2Arn":
 "arn:aws:securityhub:Region:AccountId:connectorv2/*",
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow Security Hub read access to the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "connector.securityhub.amazonaws.com"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:securityhub:Region:AccountId:connectorv2/*"
        }
    }
}
```

Edit kebijakan dengan mengganti nilai-nilai berikut dalam contoh kebijakan:

- Ganti *CloudProviderName* dengan `JIRA_CLOUD` atau `SERVICENOW`
- Ganti *AccountId* dengan ID akun tempat Anda membuat konektor Hub Keamanan.
- Ganti *Region* dengan AWS wilayah Anda (misalnya,`us-east-1`).

Akses utama IAM untuk operasi Hub Keamanan

Setiap prinsipal yang menetapkan kunci KMS yang dikelola pelanggan ke konektor Hub Keamanan harus memiliki izin untuk melakukan operasi kunci (menjelaskan, menghasilkan, mendekripsi, mengenkripsi ulang, dan mencantumkan alias) untuk kunci yang ditambahkan ke konektor. Ini berlaku untuk API CreateConnector V2 dan CreateTicket V2. Pernyataan kebijakan berikut harus disertakan sebagai bagian dari kebijakan untuk prinsipal apa pun yang berinteraksi dengan API ini.

```
{
    "Sid": "Allow permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        },
        "StringLike": {
            "kms:EncryptionContext:aws:securityhub:providerName": "CloudProviderName"
        }
    }
},
{
    "Sid": "Allow read permissions to access key through Security Hub",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::AccountId:role/RoleName"
    },
    "Action": [
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
```

```
        "StringEquals": {
            "kms:ViaService": [
                "securityhub.Region.amazonaws.com"
            ]
        }
    }
}
```

Edit kebijakan dengan mengganti nilai-nilai berikut dalam contoh kebijakan:

- Ganti *RoleName* dengan nama peran IAM yang melakukan panggilan ke Hub Keamanan.
- Ganti *CloudProviderName* dengan `JIRA_CLOUD` atau`SERVICENOW`.
- Ganti *AccountId* dengan ID akun tempat Anda membuat konektor Hub Keamanan.
- Ganti *Region* dengan AWS wilayah Anda (misalnya,`us-east-1`).

Menguji integrasi tiket yang dikonfigurasi

Untuk Jira dan ServiceNow integrasi yang dikonfigurasi, Anda dapat menguji koneksi untuk memastikan bahwa semua konfigurasi di Hub Keamanan dan di Jira atau ServiceNow lingkungan Anda selesai.

Fitur tiket tes membuat tiket dengan judul`TESTING Test CreateTicketV2 Finding`. Tiket tes diisi dengan data sampel seperti ID Akun dan wilayah akun tempat pengujian dilakukan, detail sumber daya sampel, dan contoh Men AWS cari JSON.

Menguji integrasi menggunakan konsol

Gunakan langkah-langkah berikut untuk menguji integrasi Anda:

1. Di panel navigasi Hub Keamanan pilih Integrasi.
2. Di tab Integrasi yang dikonfigurasi pilih integrasi yang ingin Anda uji.
3. Di halaman ikhtisar untuk integrasi Anda pilih Buat tiket tes.
4. Security Hub menampilkan pesan sukses dan tautan ke tiket tes jika tes berhasil. Jika pengujian tidak berhasil, Security Hub menampilkan kesalahan. Berdasarkan pesan kesalahan, atasi masalah konfigurasi di Hub Keamanan atau di ServiceNow lingkungan AndaJira.

> **Note**
>
> Fitur tiket uji dimaksudkan untuk membantu memverifikasi fungsionalitas ujung ke ujung untuk penyiapan koneksi baru atau saat Anda membuat perubahan pada koneksi yang ada. Fitur ini membuat tiket baru di Jira ServiceNow lingkungan Anda setiap kali digunakan dan tidak dimaksudkan untuk verifikasi rutin koneksi Anda.

Pengujian dengan AWS CLI

Untuk menguji integrasi Anda menggunakan AWS CLI, gunakan `create-ticket-v2` perintah dengan `--mode DRYRUN` parameter:

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region <your-region> \
  --connector-id <your-connector-id> \
  --finding-metadata-uid "TEST_FINDING"
```

Contoh

Contoh berikut menunjukkan cara menguji integrasi:

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

Respon yang Berhasil

Respons yang berhasil mengembalikan yang berikut:

```
{
    "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
```

```
    "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?
uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

`TicketSrcUrl`Dalam tanggapan memberikan tautan langsung untuk melihat tiket tes di Jira atau ServiceNow lingkungan Anda.

Jika pengujian gagal, pesan kesalahan ditampilkan yang menunjukkan masalah konfigurasi yang perlu diatasi.

Memecahkan masalah kesalahan integrasi cloud Jira

Saat menguji integrasi Anda ke Jira Cloud dari Hub Keamanan, pesan kesalahan berikut mungkin dikembalikan. Pesan kesalahan ini dapat memberikan wawasan tentang di mana masalah konfigurasi dengan konektor bisa terjadi dan bagaimana mengatasinya.

Pesan kesalahan integrasi Jira Cloud

Kesalahan	Pesan Kesalahan	Kemungkinan penyebab dan resolusi
ConflictException	Tidak dapat menemukan proyek jira	Kemungkinan penyebab: Proyek pada konektor salah, atau credentials/permissions masalah yang mencegah kami mengakses proyek. Kemungkinan resolusi: Tambahkan proyek yang benar ke konektor atau autentikasi ulang ke Jira dengan kredenSIAL yang benar.
ConflictException	Jenis masalah Hub Keamanan tidak ditemukan	Kemungkinan penyebab: Masalah penginstalan aplikasi atau jenis masalah tidak terkait dengan proyek. Kemungkinan resolusi: Lakukan langkah prasyarat untuk menginstal aplikasi Jira ke lingkungan Jira Anda dan kaitkan aplikasi dengan proyek.

Aplikasi MCP (Pratinjau)

Security Hub menyediakan pengalaman agen dengan Aplikasi Model Context Protocol (MCP). Dengan aplikasi ini, agen AI Anda dapat menyelidiki temuan eksposur. Ini juga dapat mendiagnosis konektor Azure yang ada atau menilai prasyarat konektor Azure sebelum pembuatan.

Setiap panggilan alat temuan mengembalikan ringkasan teks untuk dipertimbangkan oleh agen. Jika tersedia, itu juga mengembalikan visualisasi interaktif untuk Anda verifikasi dalam percakapan yang sama. Connector Diagnostics mengembalikan teks terstruktur yang memisahkan temuan yang dikonfirmasi dari pemeriksaan yang tidak dapat diverifikasi.

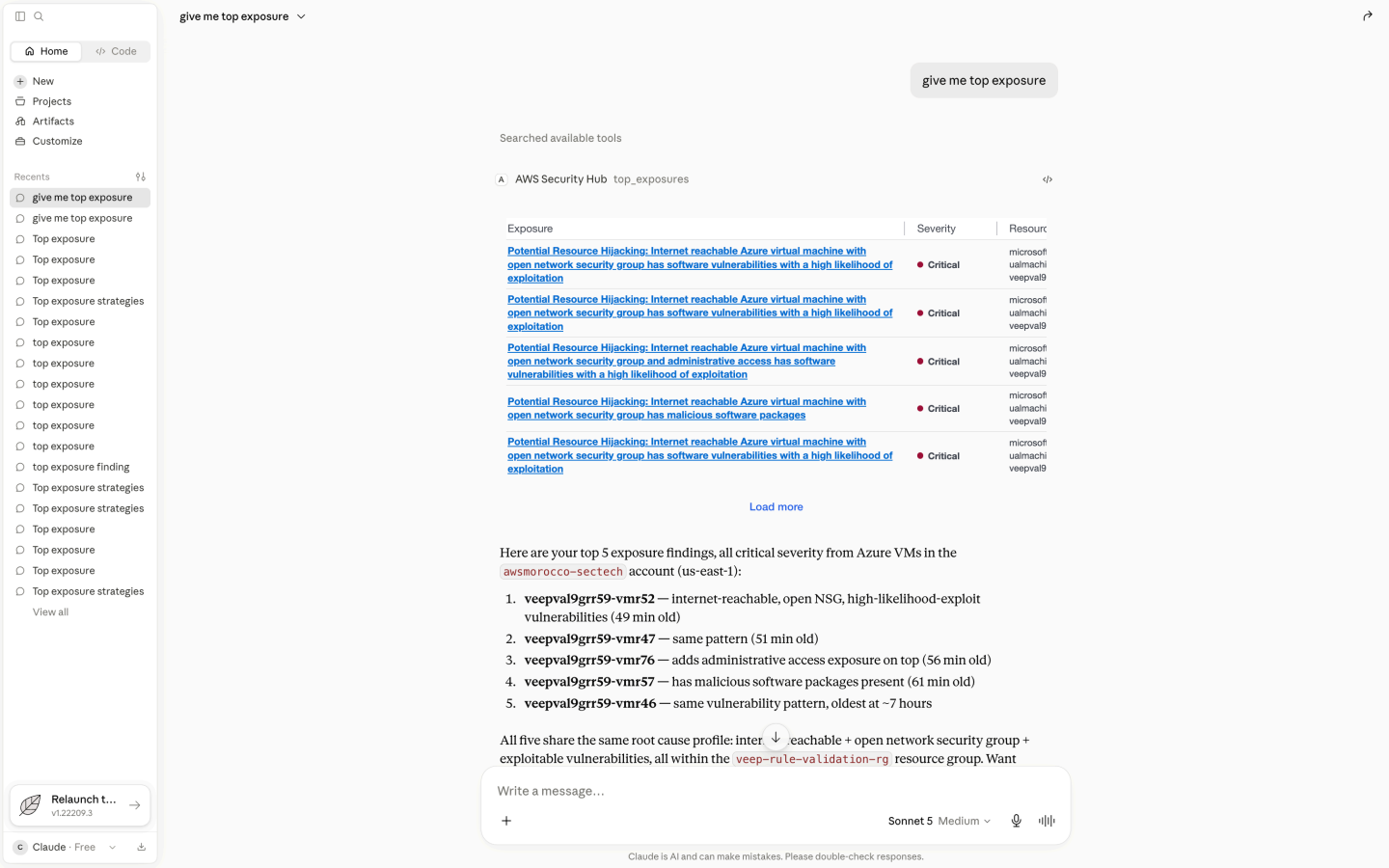
Aplikasi MCP adalah server MCP lokal yang berjalan di mesin Anda dan memanggil API Hub Keamanan secara langsung menggunakan kredenSIAL Anda yang ada AWS . Diagnostik Konektor juga dapat menjalankan kueri Azure CLI terbatas dan hanya baca menggunakan sesi Azure CLI yang ada. Setiap alat hanya dapat dibaca dan tidak mengubah postur keamanan atau sumber daya konektor Anda. Aplikasi MCP tersedia di semua Wilayah AWS komersial di mana Hub Keamanan tersedia.

> **Important**
>
> Aplikasi MCP Security Hub ada dalam pratinjau publik.

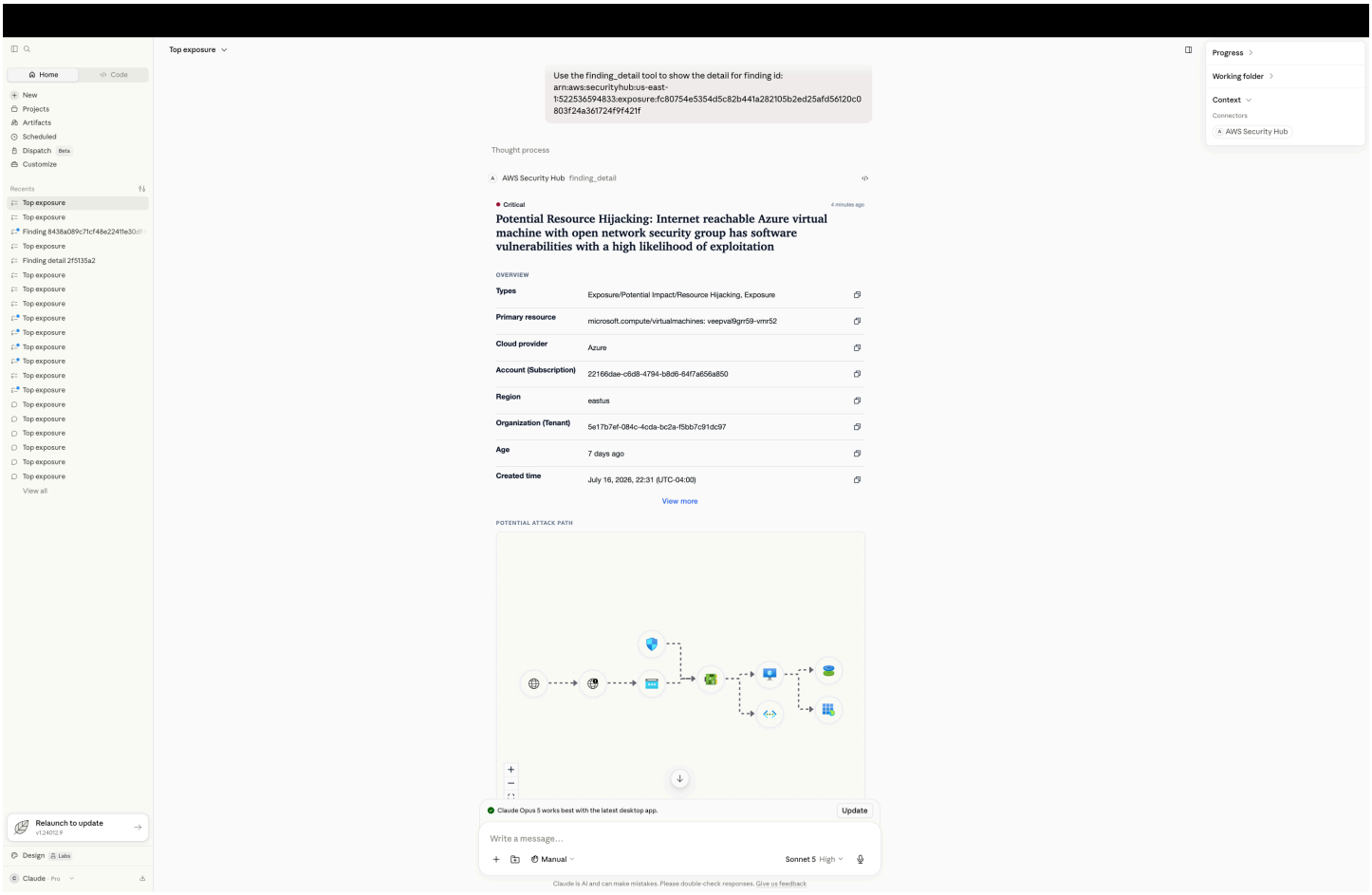
Contoh Aplikasi MCP

Contoh berikut menunjukkan bagaimana Aplikasi MCP merender visualisasi interaktif di dalam Claude Desktop saat Anda menyelidiki eksposur Anda.

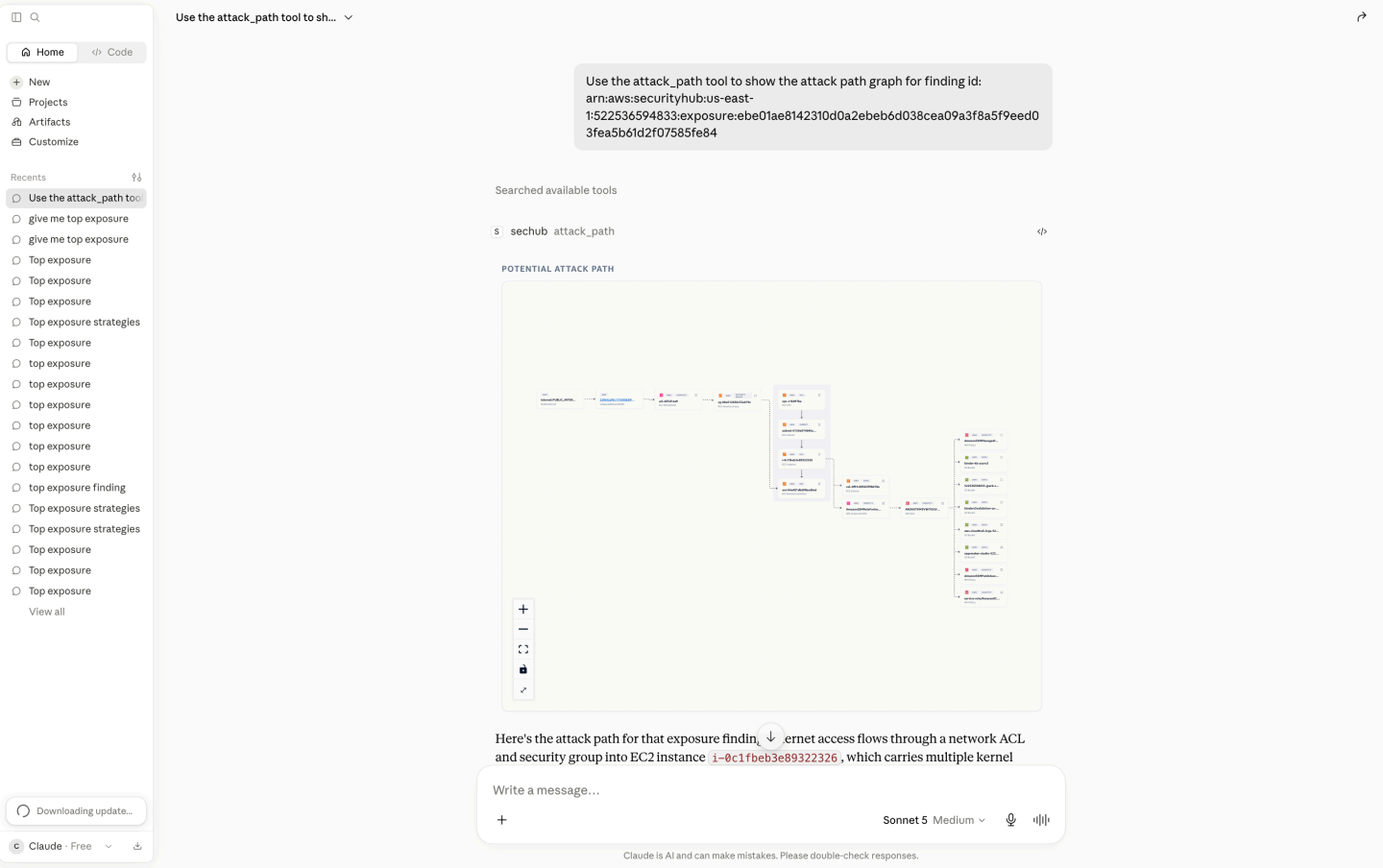
Eksposur teratas — Daftar temuan eksposur paling kritis Anda, dalam tabel interaktif. Gambar berikut menunjukkan tabel eksposur teratas.



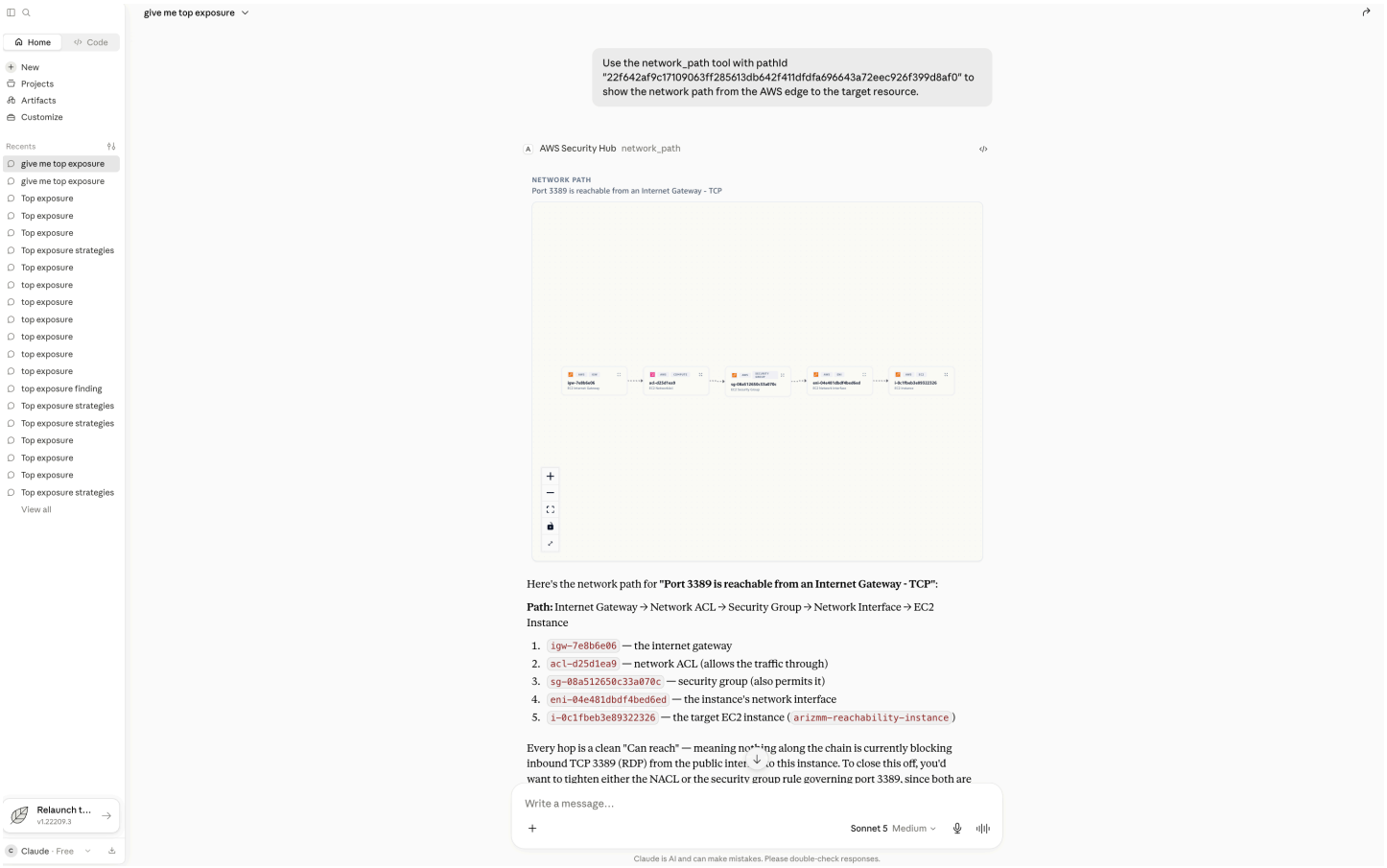
Menemukan detail — Tinjau ikhtisar temuan eksposur tunggal di samping ringkasan sifat pencarian yang berkorelasi, jalur serangan, dan panduan remediasi. Gambar berikut menunjukkan tampilan detail temuan.



Jalur serangan — Visualisasikan bagaimana eksposur dapat dijangkau sebagai grafik interaktif. Node mewakili sumber daya, identitas, dan layanan. Tepi mewakili hubungan di antara mereka. Gambar berikut menunjukkan grafik jalur serangan.



Jalur jaringan — Jelajahi lompatan jaringan yang di AWS urutkan dari tepi ke sumber daya target (misalnya, Internet Gateway ke NACL ke Grup Keamanan ke ENI ke Instance). Gambar berikut menunjukkan jalur jaringan.



Diagnosis konektor — Tanyakan mengapa konektor Azure yang ada terdegradasi atau gagal. Agen mengidentifikasi masalah yang dikonfirmasi, membedakan pemeriksaan yang tidak dapat diverifikasi, dan merekomendasikan perbaikan terkecil tanpa mengubah lingkungan Anda.

Kesiapan konektor — Periksa prasyarat Azure sebelum Anda membuat konektor. Agen melaporkan prasyarat mana yang lulus, gagal, atau tidak dapat diverifikasi.

Konsep Utama

Temuan eksposur — Temuan yang menghubungkan beberapa sinyal — seperti kerentanan, kesalahan konfigurasi, jangkauan jaringan, dan data sensitif — ke dalam satu tampilan sumber daya yang terpapar risiko.

Diagnostik Konektor — Tiga alat baca-saja untuk konektor Azure. Alat mendiagnosis konektor yang ada, menilai pengaturan yang diusulkan, dan mengambil kutipan yang tepat dari skri p pengaturan Azure yang didukung. Agen memilih alat dan menerjemahkan hasil terstrukturnya menjadi penjelasan.

Server MCP lokal — Program yang berjalan di komputer Anda dan bertindak sebagai jembatan dua arah yang aman antara Claude Desktop dan Security Hub. Server berisi alat yang digunakan agen AI Anda, termasuk alat yang membuat UI di dalam Claude Desktop. Ini menggunakan rantai AWS kredensi mesin Anda dan tidak memiliki kredensialnya sendiri.

Aplikasi MCP — Aplikasi interaktif yang dirender di dalam Claude Desktop. Setiap tampilan Aplikasi MCP melakukan satu pekerjaan, seperti menampilkan tabel eksposur teratas atau grafik jalur serangan.

Respon ganda — Panggilan alat temuan tunggal mengembalikan dua output: ringkasan teks ringkas yang ditinjau oleh agen Anda, dan visualisasi interaktif yang dirender dalam percakapan yang sama untuk Anda tinjau.

Prasyarat

- AWS Akun dengan Security Hub diaktifkan. Temuan paparan hanya diperlukan untuk temuan dan alat paparan.
- Claude Desktop diinstal. Untuk penginstal, lihat unduhan Claude Desktop di situs web Claude.
- AWS kredenSIAL dikonfigurasi dalam rantai kreden AWS sia SDK standar Anda.
- Untuk Diagnostik Azure-side Konektor, instal Azure CLI. Otentikasi ke penyewa konektor dengan menjalankan `az login --tenant`*`tenant-id`*, di *`tenant-id`* mana ID penyewa Azure yang berisi konektor. Aplikasi MCP menggunakan sesi Azure CLI lokal yang dihasilkan. Jangan menambahkan kredenSIAL Azure ke konfigurasi MCP.

> **Note**
>
> Anda dapat menjalankan Connector Diagnostics tanpa sesi Azure CLI yang diautentikasi. Hasilnya termasuk penilaian AWS sisi yang tersedia dan tanda Azure-dependent cek sebagai tidak diverifikasi. Itu tidak pernah memperlakukan bukti Azure yang tidak tersedia sebagai sehat.

Menyiapkan server MCP

Aplikasi MCP diinstal di Claude Desktop dari file bundel. Sebelum Anda menginstal, konfirmas `aws sts get-caller-identity` ikan bahwa berhasil dan `aws configure get region`

mengembalikan Wilayah di terminal Anda, sehingga server dapat membaca AWS kredenSIAL dan Wilayah Anda.

1. Unduh bundel Aplikasi MCP Security Hub.
2. Buka `.mcpb` file yang diunduh. Claude Desktop memulai aliran konfigurasi. Ikuti petunjuk untuk menginstal server.
3. Untuk memverifikasi koneksi, masukkan pertanyaan di Claude Desktop, seperti “Apa eksposur keamanan teratas saya?” atau “Konektor Azure saya di us-west-2 terdegradasi. Dapatkah Anda menentukan apa yang salah?” Jika Anda menerima kesalahan, tinjau panduan dalam pesan kesalahan dan konfirmasikan kredenSIAL dan Wilayah Anda.

Menggunakan Diagnostik Konektor

Jelaskan masalah konektor atau pengaturan yang diusulkan dalam bahasa alami. Agen memilih alat baca-saja yang sesuai, menafsirkan hasil terstrukturnya, dan memberi tahu Anda pemeriksaan mana yang dikonfirmasi dan pemeriksaan mana yang tidak diverifikasi.

Mendiagnosis konektor yang ada

1. Identifikasi konektor dengan ID konektor atau nama tepatnya. Juga berikan AWS akun dan Wilayah yang berisi konektor jika agen tidak dapat menentukannya dari permintaan Anda.
2. Ajukan pertanyaan seperti “Konektor Azure saya di us-west-2 terdegradasi. Bisakah Anda menentukan apa yang salah dan memberi tahu saya apa yang harus diperbaiki terlebih dahulu?”
3. Tinjau temuan yang dikonfirmasi secara terpisah dari pemeriksaan yang tidak diverifikasi. Ketika otentikasi Azure tidak tersedia, agen membatasi kesimpulannya pada AWS bukti sisi.

Menilai konektor yang diusulkan

1. Berikan AWS akun, Wil AWS ayah, dan ID penyewa Azure. Juga berikan 1-10 ID langganan Azure yang akan dicakup oleh konektor yang diusulkan. Beri tahu agen prasyarat layanan mana yang harus dinilai: Cloud Security Posture Management (CSPM), pemindaian Inspector VM, atau deteksi ancaman. Pilihan ini mencakup pemeriksaan kesiapan. Mereka bukan pengaturan pembuatan konektor.
2. Ajukan pertanyaan seperti “Sebelum saya membuat konektor Azure saya, periksa apakah prasyarat siap untuk langganan ini.”

3. Tinjau pemeriksaan yang lulus, gagal, dan belum diverifikasi. Hasil kesiapan yang sehat berarti bahwa prasyarat yang diperiksa lulus. Ini tidak berarti bahwa konektor ada, sedang berjalan, atau telah pulih.

Ambil instruksi penyiapan

Jika hasil mengacu pada langkah orientasi, minta agen untuk menunjukkan langkah itu. Misalnya, tanyakan “Tunjukkan langkah 6 dari skrip pengaturan konektor Azure yang didukung.” Untuk skrip lengkapnya, lihat Meng onfigurasi Microsoft Azure untuk mengintegrasikan dengan Security Hub. Alat mengembalikan kutipan yang tepat tetapi tidak menjalankannya. Jalankan skrip yang didukung lengkap karena langkah-langkahnya berbagi konfigurasi dan fungsi pembantu.

> **Note**
>
> Diagnostik Konektor tidak pernah memperbaiki atau mengubah sumber daya. Remediasi adalah panduan untuk tindakan terpisah yang Anda kendalikan. Diagnosis melaporkan pemulihan hanya ketika bukti runtime baru membuktikannya.

Alat yang tersedia

`top_exposures`— Daftar temuan eksposur Anda yang paling mendesak sebagai tabel interaktif. Panggil alat ini terlebih dahulu karena alat per-pencarian memerlukan ID pencarian dari daftar ini.

`finding_detail`— Mengembalikan ikhtisar dari satu temuan, termasuk ringkasan sifat temuan yang berkorelasi.

`finding_overview`— Mengembalikan ringkasan teks dari satu temuan dengan menemukan ID.

`correlated_finding_detail`— Daftar temuan yang berkorelasi dengan satu paparan untuk satu sifat, seperti Kerentanan, Miskonfigurasi, atau Jangkauan.

`attack_path`— Membangun grafik jalur serangan untuk satu temuan.

`network_path`— Memperluas jalur jaringan temuan menjadi lompatan terurutan dari AWS tepi ke sumber daya target.

`recommendation`— Mengembalikan panduan remediasi untuk satu temuan, termasuk tautan dokumentasi.

`resource_detail`— Mengembalikan konfigurasi satu AWS sumber daya dengan ID pendek (misalnya,`i-1234`) atau ARN.

`diagnose_connector`— Mendiagnosis konektor Azure yang ada menggunakan status Hub Keamanan dan bukti Azure CLI terbatas bila tersedia. Ini mengembalikan temuan yang dikonfirmasi, ruang lingkup yang terpengaruh, panduan remediasi, dan kesegaran data. Ini juga mencantumkan cek apa pun yang tidak dapat diverifikasi.

`assess_connector_readiness`— Menilai AWS sisi -dan Azure-side prasyarat untuk konektor Azure yang diusulkan sebelum pembuatan. Itu tidak membuat konektor.

`get_connector_setup_instructions`— Mengembalikan kutipan yang tepat dari skrip onboarding Azure yang dikemas dan didukung. Itu tidak mengeksekusi skrip.

Memantau penggunaan dan biaya di Security Hub

Halaman Penggunaan membantu Anda memahami dan mengelola biaya menjalankan Security Hub di seluruh organisasi Anda. Dari halaman ini, Anda dapat melihat biaya saat ini, melihat biaya bulanan yang diproyeksikan, menjelajahi penggunaan berdasarkan kemampuan atau akun, dan menemukan strategi untuk mengoptimalkan pengeluaran Anda.

Siapa yang dapat mengakses halaman Penggunaan

Halaman Penggunaan tersedia dari akun mana pun yang mengaktifkan Hub Keamanan. Untuk mengaksesnya, buka konsol Hub Keamanan dan pilih Penggunaan di bawah Pengaturan di panel navigasi.

> **Important**
>
> Jika akun Anda adalah akun anggota di AWS Organisasi dan administrator yang didelegasikan Hub Keamanan belum ditunjuk, data penggunaan tidak tersedia. Untuk melihat data penggunaan, akun manajemen organisasi Anda harus menunjuk administrator yang didelegasikan. Untuk informasi selengkapnya, lihat the section called “Menunjuk administrator yang didelegasikan”.

Pengalaman berbeda tergantung pada jenis akun Anda:

- Administrator atau akun manajemen yang didelegasikan — Anda melihat halaman Penggunaan lengkap dengan Ringkasan Biaya Organisasi, penggunaan berdasarkan kemampuan, penggunaan berdasarkan akun, dan strategi pengoptimalan biaya.
- Akun anggota atau akun mandiri — Anda melihat Ringkasan Biaya Akun dengan penggunaan berdasarkan kemampuan hanya untuk akun Anda. Tab Berdasarkan akun tidak tersedia karena Anda melihat satu akun.

Ringkasan biaya organisasi dan akun

> **Note**
>
> Bagian ringkasan biaya organisasi hanya terlihat dari akun administrator yang didelegasikan atau akun manajemen. Akun anggota dan akun mandiri melihat ringkasan biaya Akun sebagai gantinya.

Saat Anda membuka halaman Penggunaan dari administrator atau akun manajemen yang didelegasikan, bagian Ringkasan Biaya Organisasi menampilkan ikhtisar tingkat tinggi biaya Hub Keamanan organisasi Anda untuk siklus penagihan saat ini. Bagian ini mencakup hal-hal berikut:

- Data terakhir diseg arkan — Tanggal saat Hub Keamanan terakhir menyegarkan data penggunaan untuk organisasi Anda. Security Hub menyegarkan data ini secara berkala. Jika data berusia lebih dari 24 jam saat Anda mengunjungi halaman Penggunaan, Hub Keamanan secara otomatis memicu penyegaran. Penyegaran selesai dalam beberapa jam, tergantung pada ukuran organisasi Anda. Saat data sedang disegarkan, peringatan muncul dengan pesan bahwa data akan segera tersedia.
- Biaya saat ini — Jumlah total yang dikeluarkan organisasi Anda untuk menggunakan Hub Keamanan dari awal siklus penagihan saat ini hingga tanggal data terakhir diperbarui.
- Biaya bulanan yang diproyeksikan (30 hari) — Perkiraan biaya bulanan berdasarkan 7 hari terakhir penggunaan, diekstrapolasi ke siklus penagihan 30 hari penuh. Proyeksi ini mencakup penggunaan uji coba berbayar dan gratis untuk memberi Anda perkiraan realistis tentang seperti apa biaya bulanan Anda nantinya. Biaya yang diproyeksikan tidak memperhitungkan diskon (EDP) apa pun yang telah Anda negosi AWS asikan. Jika biaya yang diproyeksikan tampak lebih rendah dari biaya Anda saat ini, itu berarti bahwa penggunaan Anda telah menurun dan berdasarkan penggunaan 7 hari terakhir, tagihan 30 hari akan lebih rendah daripada tagihan Anda dalam siklus penagihan saat ini.

Tampilan Kemampuan

Tampilan Kemampuan menunjukkan biaya dan penggunaan Anda di seluruh organisasi, diatur berdasarkan kemampuan keamanan. Kemampuan diatur ke dalam tiga kelompok yang dapat diperluas. Anda dapat memperluas atau menciutkan setiap grup untuk melihat jenis penggunaan individual di dalamnya. Setiap jenis penggunaan dipetakan langsung ke jenis penggunaan yang sesuai di AWS Cost Explorer.

Paket esensial Security Hub — Memonitor instans EC2 Anda, gambar wadah ECR, fungsi Lambda, pengguna IAM, dan peran IAM. Meliputi analisis risiko dan eksposur, manajemen kerentanan (didukung oleh Amazon Inspector), manajemen postur keamanan (didukung oleh Security Hub CSPM), dan respons keamanan. Semua kemampuan ini disertakan dalam paket esensial dengan harga per sumber daya tunggal — Anda tidak perlu mengaktifkan atau membayar secara terpisah untuk Amazon Inspector atau AWS Security Hub CSPM, dan Anda tidak dikenakan biaya ganda untuk penggunaan layanan yang mendasarinya.

Analisis ancaman — Termasuk peristiwa CloudTrail manajemen dan peristiwa data, aktivitas jaringan, dan log lainnya. Kemampuan ini mencakup deteksi ancaman yang didukung oleh Amazon GuardDuty.

Kemampuan tambahan - Termasuk pemindaian kode fungsi Lambda. Ini adalah peningkatan opsional yang didukung oleh Amazon Inspector untuk menganalisis kode aplikasi fungsi Lambda untuk kerentanan keamanan.

Untuk informasi selengkapnya tentang harga untuk setiap kemampuan, lihat Harga Hub Keamanan.

Tabel dalam tampilan ini mencakup kolom berikut untuk setiap jenis penggunaan:

- Penggunaan saat ini — Volume penggunaan total untuk jenis penggunaan ini dari awal siklus penagihan hingga tanggal data terakhir diperbarui, di semua akun dan semua wilayah.
- Penggunaan gratis — Total volume penggunaan untuk jenis penggunaan ini dari akun yang saat ini dalam uji coba gratis. Nilai penggunaan gratis muncul dalam warna hijau.
- Biaya saat ini — Total biaya untuk jenis penggunaan ini dari awal siklus penagihan hingga tanggal data terakhir diperbarui, di semua akun dan semua wilayah.
- Nilai uji coba gratis — Biaya yang akan Anda keluarkan untuk jenis penggunaan ini jika akun yang saat ini dalam uji coba gratis tidak dalam uji coba. Ini membantu Anda memahami nilai uji coba gratis.

- Biaya bulanan yang diproyeksikan (30 hari) — Perkiraan biaya bulanan untuk jenis penggunaan ini, diekstrapolasi dari 7 hari terakhir penggunaan di semua akun dan semua wilayah. Ini termasuk penggunaan uji coba berbayar dan gratis untuk memberikan perkiraan biaya bulanan.

Tampilan Akun

> **Note**
>
> T ampilan akun hanya tersedia dari akun administrator yang didelegasikan atau akun manajemen.

Pilih tampilan akun untuk melihat biaya yang diatur berdasarkan akun anggota individual di semua wilayah. Tampilan ini membantu Anda mengidentifikasi akun mana yang menghasilkan biaya paling besar.

Tabel mencantumkan setiap akun dengan kolom berikut:

- Akun — Akun AWS ID, ditampilkan sebagai tautan yang dapat diklik. Memilih akun membuka panel rincian terperinci.
- Biaya saat ini — Total biaya untuk akun ini dari awal siklus penagihan hingga tanggal data terakhir diperbarui, di semua wilayah.
- Nilai uji coba gratis — Biaya yang akan dikeluarkan akun ini jika tidak dalam uji coba gratis.
- Biaya bulanan yang diproyeksikan (30 hari) — Perkiraan biaya bulanan untuk akun ini, diekstrapolasi dari 7 hari terakhir penggunaan di semua wilayah hingga siklus penagihan 30 hari penuh. Proyeksi mencakup penggunaan uji coba berbayar dan gratis untuk memberikan perkiraan yang representatif dari biaya bulanan Anda. Biaya yang diproyeksikan tidak memperhitungkan diskon apa pun yang telah Anda negosiasikan dengan AWS (EDP).

  Jika Security Hub diaktifkan pada akun ini dalam 7 hari terakhir, proyeksi didasarkan pada jumlah hari sejak pengaktifan. Setelah 7 hari, proyeksi menggunakan 7 hari terakhir penuh penggunaan. Halaman Penggunaan saat ini tidak mendeteksi ketika Hub Keamanan telah dinonaktifkan pada akun. Jika Security Hub baru-baru ini dinonaktifkan pada satu atau beberapa akun, akun tersebut akan terus muncul dalam proyeksi sampai penggunaannya habis. Biarkan 7 hari setelah membuat perubahan ini agar proyeksi mencerminkan status organisasi Anda yang diperbarui.

Tampilan detail akun

Ketika Anda memilih akun dari daftar, panel detail terbuka di sisi kanan halaman. Panel ini menunjukkan rincian tingkat kemampuan yang sama dengan tampilan Kemampuan, tetapi difilter ke akun tertentu. Anda dapat melihat penggunaan saat ini, penggunaan gratis, biaya saat ini, nilai uji coba gratis, dan biaya bulanan yang diproyeksikan untuk setiap jenis penggunaan dalam akun tersebut, di semua wilayah.

Strategi optimasi biaya

Pilih Strategi pengoptimalan biaya pada halaman Penggunaan untuk menavigasi ke halaman khusus dengan cara yang dapat ditindaklanjuti untuk mengelola biaya Anda sambil mempertahankan cakupan keamanan Anda.

Setiap strategi disajikan sebagai opsi independen yang dapat Anda evaluasi dan terapkan berdasarkan kebutuhan organisasi Anda. Opsi tanpa pertukaran keamanan terdaftar terlebih dahulu. Setelah menerapkan strategi apa pun, perubahan biasanya memakan waktu 24 hingga 48 jam untuk tercermin dalam penagihan Anda.

Sumber daya terkait

- Harga Security Hub
- AWS Panduan Pengguna Cost Explorer

Menonaktifkan Hub Keamanan

Menonaktifkan Hub Keamanan untuk satu akun

Jika akun Anda bukan bagian dari organisasi, Anda dapat menonaktifkan Hub Keamanan di konsol Hub Keamanan kapan saja atau menggunakan DisableSecurityHubV2 API. Saat Anda menonaktifkan Hub Keamanan, itu berhenti menelan temuan dari mesin deteksi, Anda juga kehilangan akses ke temuan, integrasi, dan konfigurasi yang ada.

Saat Anda menonaktifkan Hub Keamanan untuk akun Anda di semua Wilayah, Hub Keamanan juga menghapus Penganalisis Akses IAM yang ditautkan dengan layanan yang dibuat saat Anda mengaktifkan layanan. Jika penghapusan otomatis gagal, Anda dapat menghapus penganalisis dengan memanggil operasi `DeleteServiceLinkedAnalyzer` API Penganalisis Akses IAM.

Operasi ini berhasil hanya setelah Hub Keamanan sepenuhnya dinonaktifkan untuk akun Anda. Jika Anda menonaktifkan Hub Keamanan di satu Wilayah tetapi tetap diaktifkan di Wilayah lain, penganalisis akses yang tidak digunakan akan terus berjalan dan temuan akan terus direplikasi ke Wilayah yang diaktifkan yang tersisa.

Untuk menonaktifkan Hub Keamanan

1. Masuk ke AWS akun Anda dengan kredensional Anda, dan buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Umum.
3. Di Hub Keamanan, pilih Non aktifkan. Di jendela pop-up, masukkan**`Disable`**, dan pilih Non aktifkan.

Menonaktifkan Hub Keamanan di seluruh organisasi

Jika Anda adalah administrator yang didelegasikan untuk AWS Organisasi, Anda memiliki dua opsi untuk menonaktifkan Hub Keamanan di seluruh akun anggota.

Opsi 1: Menonaktifkan Hub Keamanan dengan mesin deteksi

Anda dapat memanfaatkan penye baran dan kebijakan Hub Keamanan (kemampuan penting dan tambahan) dari katalog kebijakan di akun administrator yang didelegasikan untuk menonaktifkan Hub Keamanan bersama dengan Amazon Inspector untuk unit organisasi, akun, atau wilayah tertentu.

Menonaktifkan Security Hub dan Amazon Inspector di seluruh akun anggota menggunakan kebijakan

1. Masuk menggunakan AWS akun Anda dengan kredensional administrator yang didelegasikan. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Konfigurasi.
3. Pilih Hub Keamanan (kemampuan penting dan tambahan) dari katalog Konfigurasi.
4. Pada halaman Konfigurasi Hub Keamanan di bagian Detail, masukkan nama dan deskripsi untuk kebijakan tersebut (misalnya, “Kebijakan Penonaktifan Hub Keamanan”).
5. Di bagian Pemilihan akun, pilih salah satu opsi berikut. Pilih Semua unit organisasi dan akun jika Anda ingin menerapkan penonaktifan ke semua unit organisasi dan akun. Pilih Unit dan akun organisasi tertentu jika Anda ingin menerapkan penonaktifan ke unit dan akun organisasi tertentu. Jika Anda memilih opsi ini, gunakan bilah pencarian atau pohon struktur organisasi untuk menentukan unit dan akun organisasi target.

6. Di bagian Wil ayah, pilih Non aktifkan semua Wilayah untuk menonaktifkan Hub Keamanan di semua Wilayah. Secara opsional pilih apakah akan secara otomatis menonaktifkan Wilayah baru. Pilih Tentukan Wilayah untuk memilih Wilayah tertentu yang ingin Anda nonaktifkan.
7. (Opsional) Untuk pengaturan lanjutan, lihat panduan dari AWS Organizations.
8. (Opsional) Untuk tag Sumber daya, tambahkan tag sebagai pasangan kunci-nilai untuk membantu Anda mengidentifikasi konfigurasi dengan mudah.
9. Pilih Berikutnya.
10. Tinjau perubahan Anda, lalu pilih Ter apkan. Akun target Anda dikonfigurasi berdasarkan kebijakan. Status konfigurasi kebijakan Anda ditampilkan di bagian atas halaman Kebijakan.

Menonaktifkan Amazon GuardDuty dan AWS Hub Keamanan CSPM

Untuk kemampuan GuardDuty dan Security Hub CSPM, Anda harus menonaktifkan kemampuan secara manual dari masing-masing akun administrator yang didelegasikan. GuardDuty dan Security Hub CSPM menggunakan penerapan (tindakan satu kali) daripada kebijakan, jadi penonaktifan harus dilakukan secara manual dari konsol masing-masing.

Opsi 2: Menonaktifkan Hub Keamanan saja

Jika Anda memiliki kebijakan Hub Keamanan yang ada dan ingin menonaktifkan Hub Keamanan saja, tanpa memengaruhi Amazon Inspector, GuardDuty, atau Security Hub CSPM, ikuti langkah-langkah berikut.

Untuk menonaktifkan Hub Keamanan hanya di seluruh akun anggota

1. Masuk menggunakan AWS akun Anda dengan kredensional administrator yang didelegasikan. Buka konsol Hub Keamanan di https://console.aws.amazon.com/securityhub/v2/home.
2. Dari panel navigasi, pilih Manajemen, lalu pilih Konfigurasi.
3. Pilih salah satu kebijakan Hub Keamanan Anda dari Kebijakan yang dikonfigurasi.
4. Pilih Edit kebijakan dan di bagian Pemilihan akun, pilih salah satu opsi berikut. Pilih Semua unit organisasi dan akun jika Anda ingin menerapkan penonaktifan ke semua unit organisasi dan akun. Pilih Unit dan akun organisasi tertentu jika Anda ingin menerapkan penonaktifan ke unit dan akun organisasi tertentu. Jika Anda memilih opsi ini, gunakan bilah pencarian atau pohon struktur organisasi untuk menentukan unit dan akun organisasi target.

5. Di bagian Wil ayah, pilih Non aktifkan semua Wilayah untuk menonaktifkan Hub Keamanan di semua Wilayah. Secara opsional pilih apakah akan secara otomatis menonaktifkan Wilayah baru. Pilih Tentukan Wilayah untuk memilih Wilayah tertentu yang ingin Anda nonaktifkan.
6. (Opsional) Untuk pengaturan lanjutan, lihat panduan dari AWS Organisasi.
7. (Opsional) Untuk tag Sumber daya, tambahkan tag sebagai pasangan kunci-nilai untuk membantu Anda mengidentifikasi konfigurasi dengan mudah.
8. Pilih Berikutnya.
9. Tinjau perubahan Anda, lalu pilih Ter apkan. Akun target Anda dikonfigurasi berdasarkan kebijakan. Status konfigurasi kebijakan Anda ditampilkan di bagian atas halaman Konfigurasi.

Dampak pada layanan keamanan lainnya

Menonaktifkan Hub Keamanan melalui kebijakan Hub Keamanan tidak berdampak pada konfigurasi CSPM GuardDuty, dan Amazon Inspector Hub.

Jika Anda perlu menonaktifkan Amazon Inspector hanya di seluruh akun anggota, Anda dapat menggunakan kebijakan manajemen kerentanan dari katalog konfigurasi Hub Keamanan. Arahkan ke halaman Konfigurasi Hub Keamanan, pilih Manajemen kerentanan dari Amazon Inspector, dan buat kebijakan nonaktifkan mengikuti langkah-langkah yang mirip dengan prosedur menonaktifkan Hub Keamanan di atas.

Keamanan diAWSSecurity Hub

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWSjuga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-partyAuditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari program AWS kepatuhan. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Security Hub, lihat AWSLayanan dalam Lingkup berdasarkan Program Kepatuhan.

- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Security Hub. Topik berikut menunjukkan cara mengonfigurasi Security Hub untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Security Hub Anda.

Topik

- Perlindungan data diAWSSecurity Hub
- AWS Manajemen Identitas dan Akses untuk Hub Keamanan
- Validasi kepatuhan untuk AWS Hub Keamanan
- Ketahanan di AWS Hub Keamanan
- Keamanan infrastruktur di AWS Hub Keamanan
- AWS Hub Keamanan dan titik akhir antarmuka VPC (AWS PrivateLink)

Perlindungan data diAWSSecurity Hub

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Security Hub. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semuaAWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data AWS . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensil dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.

- Siapkan API dan logging aktivitas pengguna denganAWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrailPanduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnyaLayanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Security Hub atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Security Hub adalah penawaran layanan multi-tenant. Untuk membantu melindungi data Anda, Security Hub mengenkripsi data saat istirahat dan data dalam perjalanan antar layanan komponen.

Memilih untuk tidak menggunakan data Anda untuk perbaikan layanan

> **Note**
>
> Halaman dokumentasi ini hanya berlaku untuk Hub AWS Keamanan yang disempurnakan yang diluncurkan pada 2 Desember 2025. Jika Anda adalah pelanggan dari Security Hub asli (sekarang AWS AWS Security Hub CSPM), penggunaan data yang dijelaskan di bawah ini hanya akan berlaku setelah Anda mengaktifkan Hub Keamanan yang disempurnakan AWS .

Anda dapat memilih untuk tidak menggunakan data Anda (didefinisikan sebagai “Konten Hub Keamanan” dalam ketentuan layanan Hub Keamanan) untuk mengembangkan dan meningkatkan Hub AWS Keamanan dan layanan AWS keamanan lainnya dengan menggunakan kebijakan opt-out

AWS Organisasi. Anda dapat memilih untuk memilih keluar meskipun Hub Keamanan saat ini tidak mengumpulkan Konten tersebut. Untuk informasi selengkapnya tentang cara memilih keluar, lihat kebijakan opt-out layanan AI di Panduan AWS Organizations Pengguna.

> **Note**
>
> Agar Anda dapat menggunakan kebijakan opt-out, AWS akun Anda harus dikelola secara terpusat oleh AWS Organisasi. Jika Anda belum membuat organisasi untuk AWS akun Anda, lihat Membuat dan mengelola organisasi di Panduan AWS Organizations Pengguna.

Memilih keluar memiliki efek sebagai berikut:

- Security Hub akan menghapus Konten yang dikumpulkan dan disimpan untuk tujuan peningkatan layanan sebelum Anda memilih keluar (jika ada).
- Setelah Anda memilih keluar, Security Hub tidak akan lagi mengumpulkan atau menyimpan Konten ini untuk tujuan peningkatan layanan.

Bagian berikut menjelaskan bagaimana Security Hub akan menangani konten Anda untuk peningkatan layanan.

AWS Penggunaan data Hub Keamanan

Saat ini, AWS Security Hub tidak mengumpulkan atau menyimpan Konten Hub Keamanan apa pun untuk tujuan peningkatan layanan. Namun, di masa mendatang, Security Hub dapat mengumpulkan dan menggunakan temuan keamanan pihak ketiga yang Anda kumpulkan di Hub Keamanan dan bentuk Konten Hub Keamanan lainnya (yang diterima Hub Keamanan dari Anda atau layanan hulu untuk tujuan menyediakan kemampuan Hub Keamanan) untuk meningkatkan Hub Keamanan dan kemampuan layanan AWS keamanan lainnya.

Kepercayaan Anda, privasi, dan keamanan Konten Anda adalah prioritas tertinggi kami. Jika Security Hub mulai mengumpulkan Konten Hub Keamanan untuk tujuan peningkatan layanan di masa mendatang, halaman ini akan diperbarui untuk mencerminkan perubahan tersebut dan memberikan rincian tentang data apa yang dikumpulkan dan bagaimana data tersebut digunakan. Anda dapat memilih keluar dari pengumpulan Konten Hub Keamanan ini kapan saja menggunakan kebijakan AWS opt-out Organisasi yang dijelaskan di atas. Untuk informasi selengkapnya tentang praktik privasi AWS data, lihat FAQ Privasi Data.

Referensi

Untuk prosedur opt-out serupa di layanan AWS keamanan lainnya, lihat:

- Memilih tidak menggunakan data Anda untuk peningkatan layanan di Panduan GuardDuty Pengguna Amazon.
- Memilih tidak menggunakan data Anda untuk peningkatan layanan di Panduan Pengguna Amazon Security Lake.

AWS Manajemen Identitas dan Akses untuk Hub Keamanan

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan di otorisasi (memiliki izin) untuk menggunakan sumber daya Hub Keamanan. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Cara kerja Security Hub dengan IAM
- Identity-based Contoh kebijakan untuk AWS Security Hub CSPM
- Service-linked peran untuk AWS Hub Keamanan
- AWSkebijakan terkelola untuk Security Hub
- Pemecahan Masalah AWS Identitas dan akses Security Hub

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Pemecahan Masalah AWS Identitas dan akses Security Hub)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Cara kerja Security Hub dengan IAM)

- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Identity-based Contoh kebijakan untuk AWS Security Hub CSPM)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredentif identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredenSIAL dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau kredenSIAL. Google/ Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS menyediakan SDK dan CLI untuk menandatangani permintaan kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredenSIAL sementara.

Identi tas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredenSIAL dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, gunakan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebagai praktik terbaik, gunakan kredenSIAL sementara alih-alih pengguna IAM dengan kredenSIAL jangka panjang.

Untuk informasi selengkapnya, lihat Memerlukan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS menggunakan kredenSIAL sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari

cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan sebaris (disematkan langsung ke dalam satu identitas) atau kebijakan ter kelola (kebijakan mandiri yang dilampirkan ke beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan sebaris yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat mengatur izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Cara kerja Security Hub dengan IAM

Sebelum Anda menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses ke Hub AWS Keamanan, pelajari fitur IAM mana yang tersedia untuk digunakan dengan Hub Keamanan.

Fitur IAM yang dapat Anda gunakan AWS Hub Keamanan

Fitur IAM	Dukungan Hub Keamanan
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Tidak
Kunci kondisi kebijakan	Ya
Daftar kontrol akses (ACL)	Tidak
Attribute-based kontrol akses (ABAC) - tag dalam kebijakan	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Service-linked peran	Ya

Untuk tampilan tingkat tinggi tentang cara Layanan AWS kerja Hub Keamanan dan lainnya dengan sebagian besar fitur IAM, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk Security Hub

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Security Hub mendukung kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat Identity-based Contoh kebijakan untuk AWS Security Hub CSPM.

Resource-based kebijakan untuk Security Hub

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Security Hub tidak mendukung kebijakan berbasis sumber daya. Anda tidak dapat melampirkan kebijakan IAM secara langsung ke sumber daya Hub Keamanan.

Tindakan kebijakan untuk Hub Keamanan

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Hub Keamanan menggunakan awalan berikut sebelum tindakan:

```
securityhub:
```

Misalnya, untuk memberikan izin pengguna untuk mengaktifkan Hub Keamanan, yang merupakan tindakan yang sesuai dengan pen `EnableSecurityHubV2` goperasian API Hub Keamanan, sertakan `securityhub:EnableSecurityHubV2` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Security Hub mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

```
"Action": "securityhub:EnableSecurityHubV2"
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma. Contoh:

```
"Action": [
      "securityhub:EnableSecurityHubV2",
      "securityhub:CreateAutomationRuleV2"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut:

```
"Action": "securityhub:Get*"
```

Namun, sebagai praktik terbaik, Anda harus membuat kebijakan yang mengikuti prinsip hak istimewa paling sedikit. Dengan kata lain, Anda harus membuat kebijakan yang hanya menyertakan izin yang diperlukan untuk melakukan tugas tertentu.

Untuk daftar tindakan Hub Keamanan, lihat Tindakan yang Ditetapkan oleh Hub AWS Keamanan di Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan tindakan Hub Keamanan, lihatIdentity-based Contoh kebijakan untuk AWS Security Hub CSPM.

Sumber daya kebijakan untuk Security Hub

Mendukung sumber daya kebijakan: Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Security Hub mendefinisikan jenis sumber daya berikut:

- Hub
- Produk
- Menemukan agregator, juga disebut sebagai agregator lintas wilayah
- Aturan otomatisasi

Anda dapat menentukan jenis sumber daya ini dalam kebijakan dengan menggunakan ARN.

Untuk daftar jenis sumber daya Hub Keamanan dan sintaks ARN untuk masing-masing, lihat Sumber Daya yang D itetapkan oleh Hub AWS Keamanan di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan untuk setiap jenis sumber daya, lihat Tindakan yang Ditetapkan oleh Hub AWS Keamanan di Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan sumber daya, lihatIdentity-based Contoh kebijakan untuk AWS Security Hub CSPM.

Kunci kondisi kebijakan untuk Hub Keamanan

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk daftar kunci kondisi Hub Keamanan, lihat Kunci Kondisi untuk Hub AWS Keamanan di Referensi O torisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana yang dapat digunakan dengan kunci kondisi, lihat Tindakan yang Ditetapkan oleh Hub AWS Keamanan. Untuk contoh kebijakan yang menggunakan kunci kondisi, lihatIdentity-based Contoh kebijakan untuk AWS Security Hub CSPM.

Daftar kontrol akses (ACL) di Hub Keamanan

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Security Hub tidak mendukung ACL, yang berarti Anda tidak dapat melampirkan ACL ke sumber daya Hub Keamanan.

Attribute-based kontrol akses (ABAC) dengan Hub Keamanan

Mendukung ABAC (tanda dalam kebijakan): Ya

Attribute-based kontrol akses (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Anda dapat melampirkan tag ke sumber daya Hub Keamanan. Anda juga dapat mengontrol akses ke sumber daya dengan memberikan informasi tag di `Condition` elemen kebijakan.

Untuk informasi tentang menandai sumber daya Hub Keamanan, lihatMenandai sumber daya Security Hub. Untuk contoh kebijakan berbasis identitas yang mengontrol akses ke sumber daya berdasarkan tag, lihat. Identity-based Contoh kebijakan untuk AWS Security Hub CSPM

Menggunakan kredenSIAL sementara dengan Security Hub

Mendukung kredensial sementara: Ya

KredenSIAL sementara menyediakan akses jangka pendek ke AWS sumber daya dan dibuat secara otomatis saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis membuat kredenSIAL sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda mendapatkan kredentif keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRole atau GetFederationToken.

Security Hub mendukung penggunaan kredenSIAL sementara.

Teruskan sesi akses untuk Security Hub

Mendukung sesi akses terusan (FAS): Ya

Sesi akses maju (FAS) menggunakan izin dari kepala sekolah yang memanggil Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Misalnya, Security Hub membuat permintaan FAS ke hilir Layanan AWS saat Anda mengintegrasikan Hub Keamanan dengan AWS Organizations dan ketika Anda menunjuk akun administrator Hub Keamanan yang didelegasikan untuk organisasi di Organisasi.

Untuk tugas lain, Hub Keamanan menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihatService-linked peran untuk AWS Hub Keamanan.

Peran layanan untuk Hub Keamanan

Security Hub tidak mengambil atau menggunakan peran layanan. Untuk melakukan tindakan atas nama Anda, Hub Keamanan menggunakan peran terkait layanan. Untuk detail tentang peran ini, lihatService-linked peran untuk AWS Hub Keamanan.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat menimbulkan masalah operasional dengan penggunaan Hub Keamanan Anda. Edit peran layanan hanya jika Hub Keamanan memberikan panduan untuk melakukannya.

Service-linked peran untuk Security Hub

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Security Hub menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihatService-linked peran untuk AWS Hub Keamanan.

Identity-based Contoh kebijakan untuk AWS Security Hub CSPM

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya CSPM Security Hub. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. Administrator harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol CSPM Security Hub
- Contoh: Izinkan pengguna untuk melihat izin mereka sendiri
- Contoh: Izinkan pengguna untuk melihat temuan
- Contoh: Izinkan pengguna membuat dan mengelola aturan otomatisasi

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Hub Keamanan di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa terendah — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkel AWS ola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui tindakan tertentu Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah

ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.

- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang memerlukan pengguna IAM atau pengguna root Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol CSPM Security Hub

Untuk mengakses AWS Security Hub CSPM konsol, Anda harus memiliki seperangkat izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya CSPM Hub Keamanan di situs Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran tersebut dapat menggunakan konsol CSPM Hub Keamanan, lampirkan juga kebijakan terkel AWS ola berikut ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Contoh: Izinkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
```

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan pengguna untuk melihat temuan

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan IAM yang memungkinkan pengguna untuk melihat temuan CSPM Hub Keamanan.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan pengguna membuat dan mengelola aturan otomatisasi

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan IAM yang memungkinkan pengguna membuat, melihat, memperbarui, dan menghapus aturan otomatisasi CSPM Security Hub. Agar kebijakan IAM ini berfungsi, pengguna harus menjadi administrator CSPM Hub Keamanan. Untuk membatasi izin — misalnya, untuk mengizinkan pengguna hanya melihat aturan otomatisasi — Anda dapat menghapus izin buat, perbarui, dan hapus.

```
{
            "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRuleV2",
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:ListAutomationRulesV2",
                "securityhub:GetAutomationRuleV2"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteAutomationRuleV2"
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked peran untuk AWS Hub Keamanan

AWS Security Hub menggunakan peran terkait layanan AWS Identity and Access Management (IAM) bernama. `AWSServiceRoleForSecurityHubV2` Peran terkait layanan ini adalah peran IAM yang ditautkan langsung ke Hub Keamanan. Ini telah ditentukan sebelumnya oleh Security Hub, dan mencakup semua izin yang diperlukan Hub Keamanan untuk memanggil AWS sumber daya lain Layanan AWS dan memantau atas nama Anda. Security Hub menggunakan peran terkait layanan ini di semua Wilayah AWS tempat di mana Hub Keamanan tersedia.

Peran terkait layanan membuat pengaturan Hub Keamanan lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Security Hub mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Hub Keamanan yang dapat mengambil peran tersebut.

Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan Anda tidak dapat melampirkan kebijakan izin tersebut ke entitas IAM lainnya.

Untuk meninjau detail peran terkait layanan, Anda dapat menggunakan konsol Hub Keamanan. Di panel navigasi, pilih Umum di bawah Peng aturan. Kemudian, di bagian Izin layanan, pilih Lihat izin layanan.

Anda dapat menghapus peran terkait layanan Hub Keamanan hanya setelah Anda menonaktifkan Hub Keamanan di semua Wilayah yang diaktifkan. Ini melindungi sumber daya Hub Keamanan Anda karena Anda tidak dapat menghapus izin untuk mengaksesnya secara tidak sengaja.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM dan cari layanan yang memiliki Ya di kolom peran. Service-linked Pilih Ya dengan tautan untuk meninjau dokumentasi peran terkait layanan untuk layanan tersebut.

Topik

- Service-linked izin peran untuk Hub Keamanan
- Membuat peran terkait layanan untuk Hub Keamanan
- Mengedit peran terkait layanan untuk Hub Keamanan
- Menghapus peran terkait layanan untuk Hub Keamanan

Service-linked izin peran untuk Hub Keamanan

Security Hub menggunakan peran terkait layanan bernama. `AWSServiceRoleForSecurityHubV2` Ini adalah peran terkait layanan yang diperlukan untuk Hub AWS Keamanan untuk mengakses sumber daya Anda. Peran terkait layanan ini memungkinkan Hub Keamanan untuk melakukan tugas-tugas seperti menerima temuan dari orang lain Layanan AWS dan mengonfigurasi AWS Config infrastruktur yang diperlukan untuk menjalankan pemeriksaan keamanan untuk kontrol. Peran terkait layanan `AWSServiceRoleForSecurityHubV2` memercayai layanan `securityhub.amazonaws.com` untuk menjalankan peran.

Per `AWSServiceRoleForSecurityHubV2` an terkait layanan menggunakan kebijakan terkelola. `AWSSecurityHubV2ServiceRolePolicy`

Anda harus memberikan izin untuk mengizinkan identitas IAM (seperti peran, grup, atau pengguna) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForSecurityHubV2` terkait layanan berhasil dibuat, identitas IAM yang Anda

gunakan untuk mengakses Hub Keamanan harus memiliki izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut untuk identitas IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Membuat peran terkait layanan untuk Hub Keamanan

Per `AWSServiceRoleForSecurityHubV2` an tertaut layanan dibuat secara otomatis saat Anda mengaktifkan Hub Keamanan untuk pertama kalinya atau Anda mengaktifkan Hub Keamanan di Wilayah yang sebelumnya tidak Anda aktifkan. Anda juga dapat membuat peran `AWSServiceRoleForSecurityHubV2` terkait layanan secara manual menggunakan konsol IAM, IAM CLI, atau IAM API. Untuk informasi selengkapnya tentang membuat peran secara manual, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM.

> **Important**
>
> Peran terkait layanan yang dibuat untuk akun administrator Hub Keamanan tidak berlaku untuk akun anggota Hub Keamanan terkait.

Mengedit peran terkait layanan untuk Hub Keamanan

Hub Keamanan tidak mengizinkan Anda mengedit peran `AWSServiceRoleForSecurityHubV2` terkait layanan. Setelah Anda membuat peran tertaut layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengubah deskripsi peran dengan menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Hub Keamanan

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, hapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif.

Saat Anda menonaktifkan Hub Keamanan, Hub Keamanan tidak secara otomatis menghapus peran `AWSServiceRoleForSecurityHubV2` terkait layanan untuk Anda. Jika Anda mengaktifkan Hub Keamanan lagi, layanan kemudian dapat mulai menggunakan peran terkait layanan yang ada lagi. Jika Anda tidak perlu lagi menggunakan Hub Keamanan, Anda dapat menghapus peran terkait layanan secara manual.

> **Important**
>
> Sebelum menghapus peran yang dit `AWSServiceRoleForSecurityHubV2` autkan layanan, Anda harus menonaktifkan Hub Keamanan terlebih dahulu di semua Wilayah tempat peran tersebut diaktifkan. Untuk informasi selengkapnya, lihat Menonaktifkan Hub Keamanan. Jika Hub Keamanan tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan gagal.

Untuk menghapus peran `AWSServiceRoleForSecurityHubV2` terkait layanan, Anda dapat menggunakan konsol IAM, IAM CLI, atau IAM API. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

AWSkebijakan terkelola untuk Security Hub

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola olehAWS. AWSKebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pemutakhiran akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWSkemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWSkebijakan terkelola: AWSSecurityHubFullAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan Security Hub. Kebijakan ini harus dilampirkan ke prinsipal sebelum mengaktifkan Security Hub secara manual untuk akun mereka. Misalnya, kepala sekolah dengan izin ini dapat melihat dan memperbarui status temuan. Mereka juga dapat mengonfigurasi wawasan khusus, mengaktifkan integrasi, dan mengaktifkan serta menonaktifkan standar dan kontrol. Prinsipal untuk akun administrator juga dapat mengelola akun anggota.

Detail izin

Kebijakan ini mencakup izin berikut:

- `securityhub`— Memungkinkan kepala sekolah akses penuh ke semua tindakan Security Hub.
- `guardduty`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang status akun di Amazon. GuardDuty
- `iam`— Memungkinkan kepala sekolah untuk membuat peran terkait layanan untuk Security Hub.
- `inspector`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang status akun di Amazon Inspector.
- `pricing`— Memungkinkan kepala sekolah untuk mendapatkan daftar harga dan produk. Layanan AWS

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubFullAccessdi Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: AWSSecurityHubReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat informasi di Security Hub. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Security Hub. Misalnya, kepala sekolah dengan izin ini dapat melihat daftar temuan yang terkait dengan akun mereka, tetapi tidak dapat mengubah status temuan. Mereka dapat melihat hasil wawasan, tetapi tidak dapat membuat atau mengonfigurasi wawasan khusus. Mereka tidak dapat mengonfigurasi kontrol atau integrasi produk.

Detail izin

Kebijakan ini mencakup izin berikut:

- `securityhub`— Memungkinkan pengguna untuk melakukan tindakan yang mengembalikan daftar item atau detail tentang item. Ini termasuk operasi API yang dimulai dengan`Get`,`List`, atau`Describe`.

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubReadOnlyAccessdi Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: AWSSecurityHubOrganizationsAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubOrganizationsAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif untuk mengaktifkan dan mengelola Security Hub untuk organisasi di. AWS Organizations Izin untuk kebijakan ini memungkinkan akun manajemen organisasi menunjuk akun administrator yang didelegasikan untuk Security Hub. Mereka juga mengizinkan akun administrator yang didelegasikan untuk mengaktifkan akun organisasi sebagai akun anggota.

Kebijakan ini hanya memberikan izin untukAWS Organizations. Akun manajemen organisasi dan akun administrator yang didelegasikan juga memerlukan izin untuk tindakan terkait. Izin ini dapat diberikan menggunakan kebijakan `AWSSecurityHubFullAccess` terkelola.

Detail izin

Kebijakan ini mencakup izin berikut:

- `organizations:ListAccounts`— Memungkinkan kepala sekolah untuk mengambil daftar akun yang merupakan bagian dari organisasi.
- `organizations:DescribeOrganization`— Memungkinkan kepala sekolah untuk mengambil informasi tentang organisasi.
- `organizations:ListRoots`— Memungkinkan kepala sekolah untuk membuat daftar akar organisasi.
- `organizations:ListDelegatedAdministrators`— Memungkinkan kepala sekolah untuk membuat daftar administrator yang didelegasikan dari suatu organisasi.
- `organizations:ListAWSServiceAccessForOrganization`— Memungkinkan kepala sekolah untuk membuat daftar Layanan AWS yang digunakan organisasi.
- `organizations:ListOrganizationalUnitsForParent`— Memungkinkan kepala sekolah untuk membuat daftar unit organisasi anak (OU) dari OU orang tua.
- `organizations:ListAccountsForParent`— Memungkinkan kepala sekolah untuk membuat daftar akun anak dari OU orang tua.
- `organizations:ListParents`— Daftar unit root atau organisasi (OU) yang berfungsi sebagai induk langsung dari OU atau akun anak yang ditentukan.
- `organizations:DescribeAccount` – Memungkinkan principal mengambil informasi tentang akun di organisasi.
- `organizations:DescribeOrganizationalUnit`— Memungkinkan kepala sekolah untuk mengambil informasi tentang OU dalam organisasi.
- `organizations:ListPolicies`— Mengambil daftar semua kebijakan dalam organisasi dari jenis tertentu.
- `organizations:ListPoliciesForTarget`— Daftar kebijakan yang secara langsung dilampirkan ke root target yang ditentukan, unit organisasi (OU), atau akun.
- `organizations:ListTargetsForPolicy`— Daftar semua akar, unit organisasi (OU), dan akun yang dilampirkan kebijakan yang ditentukan.
- `organizations:EnableAWSServiceAccess`— Memungkinkan prinsipal untuk mengaktifkan integrasi dengan Organizations.
- `organizations:RegisterDelegatedAdministrator`— Memungkinkan kepala sekolah untuk menunjuk akun administrator yang didelegasikan.
- `organizations:DeregisterDelegatedAdministrator`— Memungkinkan kepala sekolah untuk menghapus akun administrator yang didelegasikan.

- `organizations:DescribePolicy`— Mengambil informasi tentang kebijakan.
- `organizations:DescribeEffectivePolicy`— Mengembalikan isi kebijakan efektif untuk jenis kebijakan dan akun tertentu.
- `organizations:CreatePolicy`— Membuat kebijakan dari jenis tertentu yang dapat Anda lampirkan ke root, unit organisasi (OU), atau AWS akun individu.
- `organizations:UpdatePolicy`— Memperbarui kebijakan yang ada dengan nama, deskripsi, atau konten baru.
- `organizations:DeletePolicy`— Menghapus kebijakan yang ditentukan dari organisasi Anda.
- `organizations:AttachPolicy`— Melampirkan kebijakan ke root, unit organisasi (OU), atau akun individu.
- `organizations:DetachPolicy`Melepaskan kebijakan dari akar target, unit organisasi (OU), atau akun.
- `organizations:EnablePolicyType`— Mengaktifkan jenis kebijakan di root.
- `organizations:DisablePolicyType`— Menonaktifkan jenis kebijakan organisasi di root.
- `organizations:TagResource`— Menambahkan satu atau lebih tag ke sumber daya tertentu.
- `organizations:UntagResource`— Menghapus tag apa pun dengan kunci yang ditentukan dari sumber daya tertentu.
- `organizations:ListTagsForResource`— Daftar tag yang dilampirkan ke sumber daya tertentu.

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubOrganizationsAccessdi Panduan Referensi Kebijakan AWS Terkelola.

AWSkebijakan terkelola: AWSSecurityHubV2ServiceRolePolicy

Kebijakan ini memungkinkan Security Hub mengelola AWS Config aturan dan sumber daya Security Hub untuk organisasi Anda dan atas nama Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan layanan melakukan tindakan atas nama Anda. Anda dapat melampirkan kebijakan ini ke identitas-identitas IAM Anda. Untuk informasi selengkapnya, lihat the section called “Service-linked peran”.

Detail izin

Kebijakan ini mencakup izin berikut:

- `access-analyzer`— Buat dan hapus Penganalisis Akses IAM terkait layanan saat pelanggan mengaktifkan atau menonaktifkan Security Hub, daftar penganalisis untuk memverifikasi bahwa status penganalisis konsisten dengan status pemberdayaan, dan menghasilkan serta mengambil rekomendasi kebijakan untuk temuan akses yang tidak digunakan.
- `cloudwatch`— Ambil data metrik untuk mendukung kemampuan pengukuran untuk sumber daya Security Hub dan metrik kesehatan Konektor.
- `config`— Kelola perekam konfigurasi terkait layanan dan perekam konfigurasi terkait layanan pihak ketiga untuk sumber daya Security Hub, termasuk dukungan untuk perekam Config global. Buat daftar perekam konfigurasi dan dapatkan informasi konektor untuk mendukung integrasi cloud pihak ketiga.
- `ecr`— Ambil informasi tentang gambar dan repositori Amazon Elastic Container Registry untuk mendukung kemampuan pengukuran.
- `iam`— Buat peran terkait layanan berikut:AWS Config, IAM Access Analyzer di akun pelanggan, dan Amazon Inspector untuk pemindaian pihak ketiga. Ambil informasi akun untuk mendukung kemampuan pengukuran. Ambil kebijakan IAM yang ada sehingga pelanggan dapat melihat perbandingan kebijakan mereka saat ini dan penggantian hak istimewa paling sedikit yang direkomendasikan.
- `inspector2`— Buat, perbarui, hapus, dan daftar konektor Amazon Inspector dan konfigurasi pemindaian konektor untuk mendukung integrasi cloud pihak ketiga.
- `lambda`- Ambil informasi AWS Lambda fungsi untuk mendukung kemampuan pengukuran.
- `organizations`— Mengambil informasi akun dan unit organisasi (OU) untuk suatu organisasi.
- `securityhub`— Kelola konfigurasi Security Hub. Buat, perbarui, dan hapus konektor Security Hub untuk mendukung integrasi cloud pihak ketiga.
- `sts`— Dapatkan token identitas web untuk federasi identitas keluar untuk mendukung integrasi cloud pihak ketiga.
- `tag`— Mengambil informasi tentang tag sumber daya.

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubV2ServiceRolePolicydi Panduan Referensi Kebijakan AWS Terkelola.

Security Hub memperbarui keAWSkebijakan terkelola

Tabel berikut memberikan detail tentang pembaruan kebijakan AWS terkelola untuk AWS Security Hub sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang pembaruan kebijakan, berlangganan umpan RSS di halaman riwayat dokumen Security Hub.

Ubah	Deskripsi	Date
AWSSecurityHubV2ServiceRolePolicy— Kebijakan yang diperbarui	Security Hub memperbarui kebijakan untuk mendukung integrasi pihak ketiga. Pembaruan menambahkan izin berikut: mengelola perekam konfigurasi pihak ketiga, membuat dan mengelola konektor Security Hub dan Amazon Inspector, mengambil metrik kesehatan Connector dari, CloudWatch membuat peran terkait layanan Amazon Inspector untuk pemindaian pihak ketiga, dan mendapatkan token identitas web untuk federasi.	Juni 30, 2026
AWSSecurityHubV2ServiceRolePolicy— Kebijakan yang diperbarui	Security Hub memperbarui kebijakan untuk menambahkan izin IAM Access Analyzer. Pembaruan ini memungkinkan Security Hub membuat dan mengelola penganalisis yang dikelola layanan, membuat daftar penganalisis untuk memverifikasi bahwa konfigurasi penganalisis konsisten dengan status pemberdayaan, menghasilkan dan mengambil rekomendasi kebijakan untuk temuan akses yang tidak digunakan,	10 Mei 2026

Ubah	Deskripsi	Date
	dan mengambil kebijakan IAM untuk tampilan rekomendasi.	
AWSSecurityHubOrganizationsAccess— Kebijakan yang diperbarui	Security Hub memperbarui kebijakan untuk menambahkan izin guna menjelaskan kebijakan sumber daya guna mendukung fitur Security Hub. Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.	November 12, 2025
AWSSecurityHubFullAccess— Kebijakan yang diperbarui	Security Hub memperbarui kebijakan untuk menambahkan kemampuan seputar pengelolaan GuardDuty , Amazon Inspector, dan manajemen akun untuk mendukung fitur Security Hub. Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.	November 17, 2025

Ubah	Deskripsi	Date
AWSSecurityHubV2ServiceRolePolicy— Kebijakan yang diperbarui	Security Hub memperbarui kebijakan untuk menambahkan kemampuan pengukuran untuk Amazon Elastic Container RegistryAWS Lambda, Amazon CloudWatch, dan AWS Identity and Access Management untuk mendukung fitur Security Hub. Pembaruan juga menambahkan dukungan untuk AWS Config perekam global. Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.	November 5, 2025
AWSSecurityHubOrganizationsAccess – Pembaruan ke kebijakan yang ada	Security Hub menambahkan izin baru ke kebijakan. Izin memungkinkan manajemen organisasi untuk mengaktifkan dan mengelola Security Hub dan Security Hub CSPM untuk organisasi.	Juni 17, 2025
AWSSecurityHubFullAccess – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan izin baru yang memungkinkan prinsipal membuat peran terkait layanan untuk Security Hub.	Juni 17, 2025

Ubah	Deskripsi	Date
AWSSecurityHubV2ServiceRolePolicy – Kebijakan baru	Security Hub menambahkan kebijakan baru untuk memungkinkan Security Hub mengelola AWS Config aturan dan sumber daya Security Hub untuk organisasi pelanggan dan atas nama pelanggan. Security Hub dalam rilis pratinjau dan dapat berubah sewaktu-waktu.	Juni 17, 2025
AWSSecurityHubFullAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan untuk mendapatkan detail harga Layanan AWS dan produk.	April 24, 2024
AWSSecurityHubReadOnlyAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan terkelola ini dengan menambahkan kolom. `Sid`	Februari 22, 2024
AWSSecurityHubFullAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan sehingga dapat menentukan apakah Amazon GuardDuty dan Amazon Inspector diaktifkan di akun. Ini membantu pelanggan menyatukan informasi terkait keamanan dari beberapa. Layanan AWS	16 November 2023

Ubah	Deskripsi	Date
AWSSecurityHubOrganizationsAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan untuk memberikan izin tambahan guna mengizinkan akses hanya-baca ke fungsionalitas administrator yang didelegasikan. AWS Organizations Ini termasuk detail seperti root, unit organisasi (OU), akun, struktur organisasi, dan akses layanan.	16 November 2023
AWSSecurityHubOrganizationsAccess— Kebijakan baru	Security Hub CSPM menambahkan kebijakan baru yang memberikan izin yang diperlukan untuk integrasi CSPM Security Hub dengan Organizations.	15 Maret 2021
Security Hub CSPM mulai melacak perubahan	Security Hub CSPM mulai melacak perubahan untuk kebijakan yang AWS dikelola.	15 Maret 2021

Pemecahan Masalah AWS Identitas dan akses Security Hub

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Hub AWS Keamanan dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Hub Keamanan
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin akses terprogram ke Hub Keamanan
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses Hub Keamanan

- Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Hub Keamanan saya

Saya tidak berwenang untuk melakukan tindakan di Hub Keamanan

Jika member Konsol Manajemen AWS itahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang *`widget`* tetapi tidak memiliki `securityhub:`*`GetWidget`* izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *`my-example-widget`* menggunakan tindakan `securityhub:`*`GetWidget`*.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan tersebut, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Hub Keamanan.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan itu alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Hub Keamanan. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin akses terprogram ke Hub Keamanan

Pengguna memerlukan akses terprogram jika mereka ingin berinteraksi dengan AWS di luar. Konsol Manajemen AWS Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Disarankan) Gunakan kredenSIAL konsol sebagai kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Login untuk pengembangan AWS lokal di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, lihat Login untuk pengembangan AWS lokal di Panduan Refer AWS ensi SDK dan Alat.
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Meng onfigurasi AWS CLI untuk digunakan AWS IAM Identity Center di

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat otentikasi Pusat Identitas IAM di Panduan Refer AWS ensi SDK dan Alat.
IAM	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk dalam Menggunakan kredenSIAL sementara dengan AWS sumber daya di Panduan Pengguna IAM.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Tidak direkomendasikan) Gunakan kredentif jangka panjang untuk menandata ngani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk itu AWS CLI, lihat Meng autentikasi menggunakan kredentif pengguna IAM di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK dan alat, lihat Meng autentikasi menggunakan kredentif jangka panjang di Panduan Refer AWS ensi SDK dan Alat. • Untuk AWS API, lihat M engelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Hub Keamanan

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya Hub Keamanan saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Security Hub mendukung fitur-fitur ini, lihatCara kerja Security Hub dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM lainnya Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyedi Akun AWS akan akses milik pihak ketiga di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk AWS Hub Keamanan

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi ingin menggunakannya AWS untuk beban kerja yang diatur, Anda dapat mendaftar untuk AWS (lanjutan) atau mengaktifkan fitur lanjutan untuk lingkungan Anda AWS .

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup berdasarkan Program Kepatuhan dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program Kep AWS atuhan Program Jaminan .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Ketahanan di AWS Hub Keamanan

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Zona Ketersediaan, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di AWS Hub Keamanan

Sebagai layanan terkelola, AWS Security Hub dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat AWS Keamanan Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infra struktur di Security Pillar AWS Well-Architected Framework.

Anda menggunakan panggilan API yang di AWS publikasikan untuk mengakses Hub Keamanan melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Suite Cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

AWS Hub Keamanan dan titik akhir antarmuka VPC (AWS PrivateLink)

Anda dapat membuat koneksi pribadi antara VPC dan Hub AWS Keamanan dengan membuat antarmuka titik akhir VPC. Titik akhir antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses API Hub Keamanan secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi AWS Direct Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan API Hub Keamanan. Lalu lintas antara VPC dan Hub Keamanan Anda tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda. Untuk informasi selengkapnya, lihat Meng akses titik akhir VPC Layanan AWS menggunakan antarmuka di Panduan Amazon Virtual Private Cloud.

Pertimbangan untuk titik akhir VPC Security Hub

Sebelum menyiapkan titik akhir VPC antarmuka untuk Hub Keamanan, pastikan Anda meninjau prasyarat dan informasi lainnya di Panduan https://docs.aws.amazon.com/vpc/latest/privatelink/what-is-privatelink.html Amazon Virtual Private Cloud.

Security Hub mendukung melakukan panggilan ke semua tindakan API-nya dari VPC Anda.

Membuat titik akhir antarmuka VPC untuk Hub Keamanan

Anda dapat membuat titik akhir VPC untuk layanan Hub Keamanan menggunakan konsol Amazon VPC atau AWS Command Line Interface ()AWS CLI. Untuk informasi selengkapnya, lihat Membuat titik akhir VPC di Panduan Amazon Virtual Private Cloud.

Buat titik akhir VPC untuk Hub Keamanan menggunakan nama layanan berikut:

`com.amazonaws.`*`region`*`.securityhub`

Di *`region`* mana kode Wilayah untuk yang berlaku Wilayah AWS.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Hub Keamanan menggunakan nama DNS defaultnya untuk Wilayah, misalnya, `securityhub.us-east-1.amazonaws.com` untuk Wilayah AS Timur (Virginia Utara).

Membuat kebijakan titik akhir VPC untuk Hub Keamanan

Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC yang mengontrol akses ke Hub Keamanan. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir di Panduan Amazon Virtual Private Cloud.

Contoh: Kebijakan titik akhir VPC untuk tindakan Hub Keamanan

Berikut ini adalah contoh kebijakan titik akhir untuk Security Hub. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan Hub Keamanan yang terdaftar untuk semua prinsipal di semua sumber daya.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus titik akhir VPC di subnet yang dibagikan dengan Anda. Namun, Anda dapat menggunakan titik akhir VPC di subnet yang dibagikan dengan Anda. Untuk informasi tentang berbagi VPC, lihat Mem bagikan subnet VPC Anda dengan akun lain di Panduan Amazon Virtual Private Cloud.

Pencatatan panggilan API Hub Keamanan dengan CloudTrail

terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Hub Keamanan. CloudTrail menangkap panggilan API untuk Hub Keamanan sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan dari konsol

Hub Keamanan dan panggilan kode ke operasi API Hub Keamanan. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Hub Keamanan. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol di Ri wayat acara. Dengan menggunakan informasi CloudTrail yang dikumpulkan, Anda dapat menentukan permintaan yang dibuat ke Hub Keamanan, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan itu dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

Informasi Security Hub di CloudTrail

CloudTrail diaktifkan pada Anda Akun AWS saat Anda membuat akun. Ketika aktivitas acara yang didukung terjadi di Hub Keamanan, aktivitas tersebut direkam dalam suatu CloudTrail acara bersama dengan peristiwa AWS layanan lainnya di ri wayat acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun . Untuk informasi selengkapnya, lihat Melihat acara dengan CloudTrail riwayat acara.

Untuk catatan peristiwa yang sedang berlangsung di akun Anda, termasuk acara untuk Hub Keamanan, buat jejak. Jej ak CloudTrail memungkinkan pengiriman file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak pada konsol tersebut, jejak diterapkan ke semua Wilayah AWS . Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengkonfigurasi notifikasi Amazon SNS untuk CloudTrail
- M CloudTrail enerima file log dari beberapa wilayah dan Mener CloudTrail ima file log dari beberapa akun

Security Hub mendukung pencatatan semua tindakan API Hub Keamanan sebagai peristiwa dalam CloudTrail log. Untuk melihat daftar operasi Hub Keamanan, lihat Referensi API Hub Keamanan.

Ketika aktivitas untuk tindakan berikut dicatat CloudTrail, nilai untuk `responseElements` disetel ke`null`. Ini memastikan bahwa informasi sensitif tidak termasuk dalam CloudTrail log.

- `GetFindingsV2`

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan kredentif pengguna root atau AWS Identity and Access Management (IAM)
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Apakah permintaan dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Contoh: Entri file log Hub Keamanan

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateAutomationRuleV2` tindakan. Dalam contoh ini, aturan otomatisasi yang `TestAutomationRule` disebut dibuat. `Account ID`Atribut `Severity` dan ditentukan sebagai K riteria. Ketika aturan dicocokkan, `Severity` diperbarui ke Tinggi. Untuk informasi selengkapnya tentang aturan otomatisasi, lihatAturan otomatisasi di Hub Keamanan.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:Admin",
        "arn": "arn:aws:sts::555555555555:assumed-role/Admin",
        "accountId": "555555555555",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "AROA123456789EXAMPLE",
                "arn": "aarn:aws:iam::555555555555:role/Admin",
                "accountId": "555555555555",
                "userName": "Admin"
            },
            "attributes": {
                "creationDate": "2025-11-15T18:49:13Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2025-11-15T18:51:17Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateAutomationRuleV2",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.50",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Description": "Test Automation Rule",
        "Actions": [
            {
                "Type": "FINDING_FIELDS_UPDATE",
                "FindingFieldsUpdate": {
                    "SeverityId": 4
                }
            }
        ],
        "RuleStatus": "ENABLED",
        "Criteria": {
            "OcsfFindingCriteria": {
                "CompositeFilters": [
                    {
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "severity",
                                "Filter": {
                                    "Value": "Medium",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    },
                    {
```

```
                        "Operator": "OR",
                        "StringFilters": [
                            {
                                "FieldName": "cloud.account.uid",
                                "Filter": {
                                    "Value": "111122223333",
                                    "Comparison": "EQUALS"
                                }
                            }
                        ]
                    }
                ],
                "CompositeOperator": "AND"
            }
        },
        "ClientToken": "a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa",
        "RuleOrder": 61,
        "RuleName": "TestAutomationRule",
        "Tags": {}
    },
    "responseElements": {
        "RuleArn": "arn:aws:securityhub:us-west-2:555555555555:automation-rulev2/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "RuleId": "c8bc6f90-29e9-4eb7-919f-b145e44eb8ec"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "555555555555",
    "eventCategory": "Management"
}
```

Pengantar AWS Hub Keamanan CSPM

AWS Security Hub Cloud Security Posture Management (AWS Security Hub CSPM) memberi Anda pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda menilai AWS lingkungan Anda terhadap standar industri keamanan dan praktik terbaik.

AWS Security Hub CSPM mengumpulkan data keamanan di seluruh Akun AWS, Layanan AWS, dan mendukung produk pihak ketiga dan membantu Anda menganalisis tren keamanan Anda dan mengidentifikasi masalah keamanan prioritas tertinggi.

Untuk membantu Anda mengelola status keamanan organisasi Anda, Security Hub CSPM mendukung beberapa standar keamanan. Ini termasuk standar AWS Praktik Terbaik Keamanan Dasar (FSBP) yang dikembangkan oleh AWS, dan kerangka kerja kepatuhan eksternal seperti Pusat Keamanan Internet (CIS), Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), dan Institut Nasional Standar dan Teknologi (NIST). Setiap standar mencakup beberapa kontrol keamanan, yang masing-masing mewakili praktik terbaik keamanan. Security Hub CSPM menjalankan pemeriksaan terhadap kontrol keamanan dan menghasilkan temuan kontrol untuk membantu Anda menilai kepatuhan terhadap praktik terbaik keamanan.

Selain menghasilkan temuan kontrol, Security Hub CSPM juga menerima temuan dari orang lain Layanan AWS— seperti Amazon GuardDuty, Amazon Inspector, dan Amazon Macie — dan produk pihak ketiga yang didukung. Ini memberi Anda satu panel kaca ke berbagai masalah terkait keamanan. Anda juga dapat mengirim temuan CSPM Security Hub ke produk pihak ketiga yang lain Layanan AWS dan didukung.

Security Hub CSPM menawarkan fitur otomatisasi yang membantu Anda melakukan triase dan memperbaiki masalah keamanan. Misalnya, Anda dapat menggunakan aturan otomatisasi untuk memperbarui temuan penting secara otomatis ketika pemeriksaan keamanan gagal. Anda juga dapat memanfaatkan integrasi dengan Amazon EventBridge untuk memicu respons otomatis terhadap temuan tertentu.

Topik

- Manfaat Security Hub CSPM
- Mengakses Hub Keamanan CSPM
- Layanan terkait
- Security Hub CSPM uji coba gratis dan harga

- Konsep dan terminologi dalam Security Hub CSPM
- Mengaktifkan Security Hub CSPM
- Mengelola akun administrator dan anggota di Security Hub CSPM
- Memahami agregasi lintas wilayah di Security Hub CSPM
- Memahami standar keamanan di Security Hub CSPM
- Memahami kontrol keamanan di Security Hub CSPM
- Memahami integrasi di Security Hub CSPM
- Mengintegrasikan CSPM Security Hub dengan Microsoft Azure
- Membuat dan memperbarui temuan di Security Hub CSPM
- Melihat wawasan di Security Hub CSPM
- Secara otomatis memodifikasi dan bertindak atas temuan di Security Hub CSPM
- Bekerja dengan dasbor di Security Hub CSPM
- Batas regional untuk Security Hub CSPM
- Membuat sumber daya CSPM Security Hub dengan CloudFormation
- Berlangganan pengumuman CSPM Security Hub dengan Amazon SNS
- Menonaktifkan CSPM Security Hub
- Keamanan di AWS Security Hub CSPM
- Mencatat panggilan API Security Hub dengan CloudTrail

Manfaat Security Hub CSPM

Berikut adalah beberapa cara utama Security Hub CSPM membantu Anda memantau kepatuhan dan postur keamanan di seluruh lingkungan Anda AWS .

Mengurangi upaya untuk mengumpulkan dan memprioritaskan temuan

> Security Hub CSPM mengurangi upaya untuk mengumpulkan dan memprioritaskan temuan keamanan di seluruh akun dari produk terintegrasi Layanan AWS dan AWS mitra. Security Hub CSPM memproses pencarian data menggunakan AWS Security Finding Format (ASFF), format temuan standar. Ini menghilangkan kebutuhan untuk mengelola temuan dari berbagai sumber dalam berbagai format. Security Hub CSPM juga menghubungkan temuan di seluruh penyedia untuk membantu Anda memprioritaskan yang paling penting.

Pemeriksaan keamanan otomatis terhadap praktik dan standar terbaik

Security Hub CSPM secara otomatis menjalankan konfigurasi tingkat akun dan pemeriksaan keamanan yang berkelanjutan berdasarkan praktik AWS terbaik dan standar industri. Security Hub CSPM menggunakan hasil pemeriksaan ini untuk menghitung skor keamanan, dan mengidentifikasi akun dan sumber daya tertentu yang memerlukan perhatian.

Tampilan gabungan dari temuan di seluruh akun dan penyedia

Security Hub CSPM mengkonsolidasikan temuan keamanan Anda di seluruh akun dan produk penyedia dan menampilkan hasil di konsol CSPM Hub Keamanan. Anda juga dapat mengambil temuan melalui Security Hub CSPM API, AWS CLI, atau SDK. Dengan pandangan holistik tentang status keamanan Anda saat ini, Anda dapat melihat tren, mengidentifikasi potensi masalah, dan mengambil langkah-langkah perbaikan yang diperlukan.

Kemampuan untuk mengotomatiskan pencarian pembaruan dan remediasi

Anda dapat membuat aturan otomatisasi yang mengubah atau menekan temuan berdasarkan kriteria yang Anda tentukan. Security Hub CSPM juga mendukung integrasi dengan Amazon. EventBridge Untuk mengotomatiskan remediasi temuan tertentu, Anda dapat menentukan tindakan khusus yang akan diambil saat temuan dibuat. Misalnya, Anda dapat mengonfigurasi tindakan khusus untuk mengirim temuan ke sistem tiket atau ke sistem remediasi otomatis.

Mengakses Hub Keamanan CSPM

Security Hub CSPM tersedia di sebagian besar. Wilayah AWS Untuk daftar Wilayah di mana Security Hub CSPM saat ini tersedia, lihat titik akhir dan kuota CSPM Hub AWS Keamanan di. Referensi Umum AWS Untuk informasi tentang mengelola Wilayah AWS untuk Anda Akun AWS, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan AWS Account Management Referensi.

Di setiap Wilayah, Anda dapat mengakses dan menggunakan Security Hub CSPM dengan salah satu cara berikut:

Konsol CSPM Hub Keamanan

Ini Konsol Manajemen AWS adalah antarmuka berbasis browser yang dapat Anda gunakan untuk membuat dan mengelola AWS sumber daya. Sebagai bagian dari konsol tersebut, konsol CSPM Security Hub menyediakan akses ke akun CSPM Security Hub Anda, data, dan sumber daya. Anda dapat melakukan tugas CSPM Security Hub dengan menggunakan konsol CSPM Security

Hub — melihat temuan, membuat aturan otomatisasi, membuat Wilayah agregasi, dan banyak lagi.

Hub Keamanan CSPM API

Security Hub CSPM API memberi Anda akses terprogram ke akun, data, dan sumber daya CSPM Security Hub Anda. Dengan API, Anda dapat mengirim permintaan HTTPS langsung ke Security Hub CSPM. Untuk informasi tentang API, lihat Referensi AWS Security Hub API .

AWS CLI

Dengan AWS CLI, Anda dapat menjalankan perintah di baris perintah sistem Anda untuk melakukan tugas Security Hub CSPM. Dalam beberapa kasus, menggunakan baris perintah bisa lebih cepat dan lebih nyaman daripada menggunakan konsol. Baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan tugas. Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat Panduan AWS Command Line Interface Pengguna.

AWS SDK

AWS menyediakan SDK yang terdiri dari pustaka dan kode sampel untuk berbagai bahasa pemrograman dan platform — misalnya, Java, Go, Python, C++, dan .NET. SDK menyediakan akses terprogram yang nyaman ke Security Hub CSPM dan lainnya Layanan AWS dalam bahasa pilihan Anda. SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang menginstal dan menggunakan AWS SDK, lihat Alat untuk Membangun. AWS

Important

Security Hub CSPM hanya mendeteksi dan mengkonsolidasikan temuan yang dihasilkan setelah Anda mengaktifkan Security Hub CSPM. Ini tidak secara retroaktif mendeteksi dan mengkonsolidasikan temuan keamanan yang dihasilkan sebelum Anda mengaktifkan CSPM Hub Keamanan.

Security Hub CSPM hanya menerima dan memproses temuan di Wilayah tempat Anda mengaktifkan Security Hub CSPM di akun Anda.

Untuk kepatuhan penuh dengan pemeriksaan keamanan CIS Foun AWS dations Benchmark, Anda harus mengaktifkan Security Hub CSPM di semua Wilayah yang didukung AWS .

Layanan terkait

Untuk lebih mengamankan AWS lingkungan Anda, pertimbangkan untuk menggunakan yang lain Layanan AWS dalam kombinasi dengan Security Hub CSPM. Beberapa Layanan AWS mengirim temuan mereka ke Security Hub CSPM, dan Security Hub CSPM menormalkan temuan ke dalam format standar. Beberapa juga Layanan AWS dapat menerima temuan dari Security Hub CSPM.

Untuk daftar orang lain Layanan AWS yang mengirim atau menerima temuan CSPM Security Hub, lihat. Layanan AWS integrasi dengan Security Hub CSPM

Security Hub CSPM menggunakan aturan terkait layanan AWS Config untuk menjalankan pemeriksaan keamanan untuk sebagian besar kontrol. Kontrol mengacu pada spesifik Layanan AWS dan AWS sumber daya. Untuk daftar kontrol CSPM Security Hub, lihat. Referensi kontrol untuk Security Hub CSPM Anda harus mengaktifkan AWS Config dan merekam sumber daya AWS Config untuk Security Hub CSPM untuk menghasilkan sebagian besar temuan kontrol. Untuk informasi selengkapnya, lihat Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config.

Security Hub CSPM uji coba gratis dan harga

Saat Anda mengaktifkan Security Hub CSPM Akun AWS untuk pertama kalinya, akun tersebut secara otomatis terdaftar dalam uji coba gratis Security Hub CSPM selama 30 hari.

Saat menggunakan Security Hub CSPM selama uji coba gratis, Anda dikenakan biaya untuk penggunaan layanan lain yang berinteraksi dengan Security Hub CSPM, seperti item. AWS Config Anda tidak dikenakan biaya untuk AWS Config aturan yang diaktifkan hanya oleh standar keamanan Security Hub CSPM.

Anda tidak dikenakan biaya untuk menggunakan Security Hub CSPM sampai uji coba gratis Anda berakhir.

Melihat detail penggunaan

Security Hub CSPM menyediakan informasi penggunaan, termasuk jumlah pemeriksaan keamanan dan temuan yang diproses oleh akun Anda. Rincian penggunaan juga mencakup waktu yang tersisa dalam uji coba gratis. Informasi ini dapat membantu Anda memahami penggunaan CSPM Security Hub setelah uji coba gratis berakhir. Informasi penggunaan juga tersedia setelah uji coba gratis berakhir.

Untuk menampilkan informasi penggunaan (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Penggunaan di bawah Peng aturan.

Informasi penggunaan hanya untuk akun saat ini dan Wilayah saat ini. Di Wilayah agregasi, informasi penggunaan tidak menyertakan Wilayah yang ditautkan. Untuk informasi selengkapnya tentang Wilayah yang ditautkan, lihatthe section called “Jenis data yang dikumpulkan”.

Untuk melihat detail biaya untuk akun Anda, gunakan konsol Pen AWS agihan.

Detail harga

Untuk informasi selengkapnya tentang cara CSPM Security Hub mengenakan biaya untuk temuan yang dicari dan pemeriksaan keamanan, lihat Harga CSPM Hub Keamanan.

Konsep dan terminologi dalam Security Hub CSPM

Di AWS Security Hub CSPM, kami membangun AWS konsep dan terminologi umum dan menggunakan istilah tambahan ini.

Akun

Akun Amazon Web Services (AWS) standar yang berisi AWS sumber daya Anda. Anda dapat masuk AWS dengan akun Anda dan mengaktifkan Security Hub CSPM.

Akun dapat mengundang akun lain untuk mengaktifkan Security Hub CSPM dan dikaitkan dengan akun tersebut di Security Hub CSPM. Menerima undangan keanggotaan bersifat opsional. Jika undangan diterima, akun tersebut menjadi akun administrator, dan akun yang ditambahkan adalah akun anggota. Akun administrator dapat melihat temuan di akun anggota mereka.

Jika Anda terdaftar AWS Organizations, maka organisasi Anda menunjuk akun administrator CSPM Hub Keamanan untuk organisasi tersebut. Akun administrator CSPM Security Hub dapat mengaktifkan akun organisasi lain sebagai akun anggota.

Akun tidak dapat menjadi akun administrator dan akun anggota secara bersamaan. Akun hanya dapat memiliki satu akun administrator.

Untuk informasi selengkapnya, lihat Mengelola akun administrator dan anggota di Security Hub CSPM.

Akun Administrator

Akun di Security Hub CSPM yang diberikan akses untuk melihat temuan untuk akun anggota terkait.

Akun menjadi akun administrator dengan salah satu cara berikut:

- Akun mengundang akun lain untuk dikaitkan dengannya di Security Hub CSPM. Ketika akun tersebut menerima undangan, mereka menjadi akun anggota, dan akun undangan menjadi akun administrator mereka.
- Akun tersebut ditetapkan oleh akun manajemen organisasi sebagai akun administrator CSPM Security Hub. Akun administrator CSPM Security Hub dapat mengaktifkan akun organisasi apa pun sebagai akun anggota, dan juga dapat mengundang akun lain untuk menjadi akun anggota.

Akun hanya dapat memiliki satu akun administrator. Akun tidak dapat menjadi akun administrator dan akun anggota secara bersamaan.

Wilayah Agregasi

Mengatur Wilayah agregasi memungkinkan Anda untuk melihat temuan keamanan dari beberapa Wilayah AWS dalam satu panel kaca.

Wilayah agregasi adalah Wilayah tempat Anda melihat dan mengelola temuan. Temuan digabungkan ke Wilayah agregasi dari Wilayah terkait. Pembaruan temuan direplikasi di seluruh Wilayah.

Di Wilayah agregasi, halaman Standar Keamanan, Wawasan, dan Temuan menyertakan data dari semua Wilayah yang ditautkan.

Untuk informasi selengkapnya, lihat the section called “Menggabungkan data di seluruh Wilayah”.

Temuan yang diarsipkan

Sebuah temuan yang status catatannya (`RecordState`) adalah`ARCHIVED`. Mengarsipkan temuan menunjukkan bahwa penyedia temuan percaya bahwa temuan itu tidak lagi relevan. Status rekaman berbeda dari status alur kerja, yang melacak status penyelidikan ke dalam temuan.

Penyedia pencarian dapat menggunakan pen BatchImportFindings goperasian Security Hub CSPM API untuk mengarsipkan temuan yang mereka buat. Security Hub CSPM secara otomatis mengarsipkan temuan kontrol yang memenuhi kriteria tertentu. Untuk informasi selengkapnya, lihat Menghasilkan, memperbarui, dan mengarsipkan temuan kontrol.

Pada konsol CSPM Security Hub, pengaturan filter default mengecualikan temuan yang diarsipkan dari menemukan daftar dan tabel. Anda dapat memperbarui pengaturan untuk menyertakan temuan yang diarsipkan. Jika Anda mengambil temuan dengan menggunakan GetFindings operasi Security Hub CSPM API, operasi akan mengambil temuan yang diarsipkan dan yang aktif. Untuk mengecualikan temuan yang diarsipkan, Anda dapat memfilter hasilnya. Contoh:

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS Format Penemuan Keamanan (ASFF)

Format standar untuk isi temuan yang dikumpulkan atau dihasilkan oleh Security Hub CSPM. Format AWS Penemuan Keamanan memungkinkan Anda menggunakan Security Hub CSPM untuk melihat dan menganalisis temuan yang dihasilkan oleh layanan AWS keamanan, solusi pihak ketiga, atau Security Hub CSPM sendiri dari menjalankan pemeriksaan keamanan. Untuk informasi selengkapnya, lihat AWS Format Penemuan Keamanan (ASFF).

Kontrol

Perlindungan atau penanggulangan yang ditentukan untuk sistem informasi atau organisasi yang dirancang untuk melindungi kerahasiaan, integritas, dan ketersediaan informasinya dan untuk memenuhi serangkaian persyaratan keamanan yang ditentukan. Standar keamanan dikaitkan dengan kumpulan kontrol.

Istil ah kontrol keamanan mengacu pada kontrol yang memiliki ID kontrol tunggal dan judul di seluruh standar. Istil ah kontrol standar mengacu pada kontrol yang memiliki ID dan judul kontrol khusus standar. Saat ini, Security Hub CSPM mendukung kontrol standar hanya di Wilayah China dan. AWS GovCloud (US) Regions Kontrol keamanan didukung di semua Wilayah lainnya.

Tindakan kustom

Mekanisme CSPM Security Hub untuk mengirim temuan yang dipilih ke. EventBridge Tindakan khusus dibuat di Security Hub CSPM. Ini kemudian dikaitkan dengan EventBridge aturan. Aturan mendefinisikan tindakan tertentu yang harus diambil ketika temuan diterima yang terkait dengan ID tindakan kustom. Tindakan khusus dapat digunakan, misalnya, untuk mengirim temuan

tertentu, atau serangkaian kecil temuan, ke alur kerja respons atau remediasi. Untuk informasi selengkapnya, lihat the section called “Membuat tindakan kustom”.

Akun administrator yang didelegasikan (Organisasi)

Di AWS Organizations, akun administrator yang didelegasikan untuk layanan dapat mengelola penggunaan layanan untuk organisasi.

Di Security Hub CSPM, akun administrator CSPM Hub Keamanan juga merupakan akun administrator yang didelegasikan untuk Security Hub CSPM. Saat akun manajemen organisasi pertama kali menunjuk akun administrator CSPM Security Hub, Security Hub CSPM memanggil Organisasi untuk menjadikan akun tersebut sebagai akun administrator yang didelegasikan.

Akun manajemen organisasi kemudian harus memilih akun administrator yang didelegasikan sebagai akun administrator CSPM Hub Keamanan di semua Wilayah.

Temuan

Catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Security Hub CSPM menghasilkan dan memperbarui temuan setelah menyelesaikan pemeriksaan keamanan untuk kontrol. Ini disebut temuan kontrol. Temuan juga dapat berasal dari integrasi dengan produk lain Layanan AWS dan pihak ketiga.

Untuk informasi selengkapnya, lihat the section called “Temuan ”.

Cross-Region agregasi

Agregasi temuan, wawasan, status kepatuhan kontrol, dan skor keamanan dari Wilayah tertaut ke Wilayah agregasi. Anda kemudian dapat melihat semua data Anda dari Wilayah agregasi dan memperbarui temuan dan wawasan dari Wilayah agregasi.

Untuk informasi selengkapnya, lihat the section called “Menggabungkan data di seluruh Wilayah”.

Menemukan konsumsi

Impor temuan ke Security Hub CSPM dari AWS layanan lain dan dari penyedia mitra pihak ketiga.

Menemukan peristiwa konsumsi mencakup temuan baru dan pembaruan untuk temuan yang ada.

Wawasan

Kumpulan temuan terkait yang ditentukan oleh pernyataan agregasi dan filter opsional. Wawasan mengidentifikasi area keamanan yang membutuhkan perhatian dan intervensi. Security Hub CSPM menawarkan beberapa wawasan terkelola (default) yang tidak dapat Anda

modifikasi. Anda juga dapat membuat wawasan CSPM Security Hub khusus untuk melacak masalah keamanan yang unik untuk AWS lingkungan dan penggunaan Anda. Untuk informasi selengkapnya, lihat the section called “Wawasan”.

Wilayah Terkait

Bila Anda mengaktifkan agregasi lintas wilayah, Wilayah tertaut adalah wilayah yang menggabungkan temuan, wawasan, status kepatuhan kontrol, dan skor keamanan ke Wilayah agregasi.

Di Wilayah yang ditautkan, halaman Temuan dan Wawasan hanya berisi temuan dari Wilayah tersebut.

Untuk informasi selengkapnya, lihat the section called “Menggabungkan data di seluruh Wilayah”.

Akun Anggota

Akun yang telah memberikan izin kepada akun administrator untuk melihat dan mengambil tindakan atas temuan mereka.

Akun menjadi akun anggota dengan salah satu cara berikut:

- Akun menerima undangan dari akun lain.
- Untuk akun organisasi, akun administrator CSPM Security Hub mengaktifkan akun sebagai akun anggota.

Persyaratan terkait

Satu set persyaratan industri atau peraturan yang dipetakan ke kontrol.

Aturan

Satu set kriteria otomatis yang digunakan untuk menilai apakah kontrol dipatuhi. Ketika sebuah aturan dievaluasi, itu bisa lulus atau gagal. Jika evaluasi tidak dapat menentukan apakah aturan lulus atau gagal, maka aturan tersebut dalam keadaan peringatan. Jika aturan tidak dapat dievaluasi, maka itu dalam keadaan tidak tersedia.

Pemeriksaan keamanan

Evaluasi titik waktu tertentu dari aturan terhadap sumber daya tunggal yang menghasilkan`PASSED`,, `FAILED`, `WARNING`, atau `NOT_AVAILABLE` status. Menjalankan pemeriksaan keamanan menghasilkan temuan.

Akun administrator CSPM Hub Keamanan

Akun organisasi yang mengelola keanggotaan Security Hub CSPM untuk organisasi.

Akun manajemen organisasi menunjuk akun administrator CSPM Hub Keamanan di setiap Wilayah. Akun manajemen organisasi harus memilih akun administrator CSPM Security Hub yang sama di semua Wilayah.

Akun administrator CSPM Hub Keamanan juga merupakan akun administrator yang didelegasikan untuk Security Hub CSPM di Organisasi.

Akun administrator CSPM Security Hub dapat mengaktifkan akun organisasi apa pun sebagai akun anggota. Akun administrator CSPM Security Hub juga dapat mengundang akun lain untuk menjadi akun anggota.

Standar keamanan

Pernyataan yang diterbitkan tentang topik yang menentukan karakteristik, biasanya terukur dan dalam bentuk kontrol, yang harus dipenuhi atau dicapai untuk kepatuhan. Standar keamanan dapat didasarkan pada kerangka peraturan, praktik terbaik, atau kebijakan internal perusahaan. Kontrol dapat dikaitkan dengan satu atau lebih standar yang didukung di Security Hub CSPM. Untuk mempelajari lebih lanjut tentang standar keamanan di Security Hub CSPM, lihat. Memahami standar keamanan di Security Hub CSPM

Kepelikan

Tingkat keparahan yang ditetapkan untuk kontrol CSPM Security Hub mengidentifikasi pentingnya kontrol. Tingkat keparahan kontrol dapat berupa K ritis, Tinggi, Sedang, Rendah, atau Informasi. Tingkat keparahan yang ditetapkan untuk temuan kontrol sama dengan tingkat keparahan kontrol itu sendiri. Untuk mempelajari cara Security Hub CSPM menetapkan tingkat keparahan pada kontrol, lihat. Tingkat keparahan untuk temuan kontrol

Status alur kerja

Status penyelidikan terhadap temuan. Ini dilacak menggunakan `Workflow.Status` atribut.

Status alur kerja awalnya`NEW`. Jika Anda memberi tahu pemilik sumber daya untuk mengambil tindakan pada temuan, Anda dapat mengatur status alur kerja ke`NOTIFIED`. Jika temuan tidak menjadi masalah, dan tidak memerlukan tindakan apa pun, setel status alur kerja ke`SUPPRESSED`. Setelah Anda meninjau dan memperbaiki temuan, setel status alur kerja ke`RESOLVED`.

Secara default, sebagian besar daftar pencarian hanya menyertakan temuan dengan status alur kerja `NEW` atau`NOTIFIED`. Menemukan daftar untuk kontrol juga mencakup `RESOLVED` temuan.

Untuk GetFindings operasi, Anda dapat menyertakan filter untuk status alur kerja.

```
"WorkflowStatus": [
```

```
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Konsol Security Hub CSPM menyediakan opsi untuk mengatur status alur kerja untuk temuan. Pelanggan (atau SIEM, ticketing, manajemen insiden, atau alat SOAR yang bekerja atas nama pelanggan untuk memperbarui temuan dari penyedia pencarian) juga dapat digunakan BatchUpdateFindings untuk memperbarui status alur kerja.

Mengaktifkan Security Hub CSPM

Ada dua cara untuk mengaktifkan AWS Security Hub CSPM, dengan mengintegrasikan dengan AWS Organizations atau secara manual.

Kami sangat menyarankan untuk mengintegrasikan dengan Organisasi untuk lingkungan multi-akun dan Multi-wilayah. Jika Anda memiliki akun mandiri, Anda perlu mengatur Security Hub CSPM secara manual.

Memverifikasi izin yang diperlukan

Setelah mendaftar ke Amazon Web Services (AWS), Anda harus mengaktifkan Security Hub CSPM untuk menggunakan kemampuan dan fiturnya. Untuk mengaktifkan Security Hub CSPM, pertama-tama Anda harus mengatur izin yang memungkinkan Anda mengakses konsol CSPM Security Hub dan operasi API. Anda atau AWS administrator dapat melakukan ini dengan menggunakan AWS Identity and Access Management (IAM) untuk melampirkan kebijakan terkel AWS ola yang dipanggil `AWSSecurityHubFullAccess` ke identitas IAM Anda.

Untuk mengaktifkan dan mengelola Security Hub CSPM melalui integrasi Organisasi, Anda juga harus melampirkan kebijakan terkel AWS ola yang disebut. `AWSSecurityHubOrganizationsAccess`

Untuk informasi selengkapnya, lihat AWS kebijakan terkelola untuk Security Hub.

Mengaktifkan Security Hub CSPM dengan integrasi Organisasi

Untuk mulai menggunakan Security Hub CSPM dengan AWS Organizations, akun AWS Organizations manajemen untuk organisasi menunjuk akun sebagai akun administrator CSPM Hub

Keamanan yang didelegasikan untuk organisasi. Security Hub CSPM secara otomatis diaktifkan di akun administrator yang didelegasikan di Wilayah saat ini.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menunjuk administrator yang didelegasikan.

Security Hub CSPM console

Untuk menunjuk administrator CSPM Hub Keamanan yang didelegasikan saat onboarding

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Buka Hub Keamanan CSPM. Anda akan diminta untuk masuk ke akun manajemen Organisasi.
3. Pada halaman T entukan administrator yang didelegasikan, di bagian Akun administrator yang di delegasikan, tentukan akun administrator yang didelegasikan. Sebaiknya pilih administrator delegasi yang sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya.
4. Pilih Tet apkan administrator yang didelegasikan.

Security Hub CSPM API

Memanggil `EnableOrganizationAdminAccount` API dari akun manajemen Organisasi. Berikan Akun AWS ID akun administrator yang didelegasikan CSPM Hub Keamanan.

AWS CLI

Jalan `enable-organization-admin-account` kan perintah dari akun manajemen Organisasi. Berikan Akun AWS ID akun administrator yang didelegasikan CSPM Hub Keamanan.

Contoh perintah:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Untuk informasi selengkapnya tentang integrasi dengan Organisasi, lihatMengintegrasikan CSPM Security Hub denganAWS Organizations.

Konfigurasi pusat

Saat mengintegrasikan Security Hub CSPM dan Organisasi, Anda memiliki opsi untuk menggunakan fitur yang disebut konfigurasi pusat untuk mengatur dan mengelola Security Hub CSPM untuk organisasi Anda. Kami sangat menyarankan menggunakan konfigurasi pusat karena memungkinkan administrator menyesuaikan cakupan keamanan untuk organisasi. Jika sesuai, administrator yang didelegasikan dapat mengizinkan akun anggota untuk mengonfigurasi pengaturan cakupan keamanannya sendiri.

Konfigurasi pusat memungkinkan administrator yang didelegasikan mengonfigurasi Security Hub CSPM di seluruh akun, OU, dan. Wilayah AWS Administrator yang didelegasikan mengonfigurasi Security Hub CSPM dengan membuat kebijakan konfigurasi. Dalam kebijakan konfigurasi, Anda dapat menentukan pengaturan berikut:

- Apakah Security Hub CSPM diaktifkan atau dinonaktifkan
- Standar keamanan mana yang diaktifkan dan dinonaktifkan
- Kontrol keamanan mana yang diaktifkan dan dinonaktifkan
- Apakah akan menyesuaikan parameter untuk kontrol tertentu

Sebagai administrator yang didelegasikan, Anda dapat membuat kebijakan konfigurasi tunggal untuk seluruh organisasi atau kebijakan konfigurasi yang berbeda untuk berbagai akun dan OU Anda. Misalnya, akun pengujian dan akun produksi dapat menggunakan kebijakan konfigurasi yang berbeda.

Akun anggota dan OU yang menggunakan kebijakan konfigurasi dikelola secara terpusat dan hanya dapat dikonfigurasi oleh administrator yang didelegasikan. Administrator yang didelegasikan dapat menetapkan akun anggota tertentu dan OU sebagai pengelola sendiri untuk memberi anggota kemampuan untuk mengonfigurasi pengaturannya sendiri Region-by-Region berdasarkan basis.

Jika Anda tidak menggunakan konfigurasi pusat, sebagian besar Anda harus mengkonfigurasi Security Hub CSPM secara terpisah di setiap akun dan Wilayah. Ini disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan dapat secara otomatis mengaktifkan Security Hub CSPM dan serangkaian standar keamanan terbatas di akun organisasi baru di Wilayah saat ini. Konfigurasi lokal tidak berlaku untuk akun organisasi yang ada atau ke Wilayah selain Wilayah saat ini. Konfigurasi lokal juga tidak mendukung penggunaan kebijakan konfigurasi.

Mengaktifkan Security Hub CSPM secara manual

Anda harus mengaktifkan Security Hub CSPM secara manual jika Anda memiliki akun mandiri, atau jika Anda tidak mengintegrasikan dengan. AWS Organizations Akun mandiri tidak dapat diintegrasikan dengan AWS Organizations dan harus menggunakan pengaktifan manual.

Saat Anda mengaktifkan Security Hub CSPM secara manual, Anda menetapkan akun administrator CSPM Hub Keamanan dan mengundang akun lain untuk menjadi akun anggota. Hubungan administrator-anggota terbentuk ketika akun calon anggota menerima undangan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan Security Hub CSPM. Saat Anda mengaktifkan Security Hub CSPM dari konsol, Anda juga memiliki opsi untuk mengaktifkan standar keamanan yang didukung.

Security Hub CSPM console

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Saat Anda membuka konsol CSPM Security Hub untuk pertama kalinya, pilih Buka CSPM Hub Keamanan.
3. Pada halaman selamat datang, bagian Standar keamanan mencantumkan standar keamanan yang didukung Security Hub CSPM.

   Pilih kotak centang untuk standar untuk mengaktifkannya, dan kosongkan kotak centang untuk menonaktifkannya.

   Anda dapat mengaktifkan atau menonaktifkan standar atau kontrol individualnya kapan saja. Untuk informasi tentang mengelola standar keamanan, lihatMemahami standar keamanan di Security Hub CSPM.
4. Pilih Aktifkan Hub Keamanan.

Security Hub CSPM API

Memanggil `EnableSecurityHub` API. Saat Anda mengaktifkan Security Hub CSPM dari API, secara otomatis mengaktifkan standar keamanan default berikut:

- AWS Praktik Terbaik Keamanan Dasar
- Pusat Keamanan Internet (CIS) Dasar Ben AWS chmark v1.2.0

Jika Anda tidak ingin mengaktifkan standar ini, maka setel `EnableDefaultStandards` kefalse.

Anda juga dapat menggunakan `Tags` parameter untuk menetapkan nilai tag ke sumber daya hub.

AWS CLI

Jalankan perintah `enable-security-hub`. Untuk mengaktifkan standar default, sertakan`--enable-default-standards`. Untuk tidak mengaktifkan standar default, sertakan`--no-enable-default-standards`. Standar keamanan default adalah sebagai berikut:

- AWS Praktik Terbaik Keamanan Dasar
- Pusat Keamanan Internet (CIS) Dasar Ben AWS chmark v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

Contoh

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

Multi-account skrip pengaktifan

> **Note**
>
> Alih-alih skrip ini, sebaiknya gunakan konfigurasi pusat untuk mengaktifkan dan mengkonfigurasi Security Hub CSPM di beberapa akun dan Wilayah.

Skrip pengaktifan multi-akun CSPM Hub Keamanan GitHub memungkinkan Anda mengaktifkan CSPM Hub Keamanan di seluruh akun dan Wilayah. Skrip juga mengotomatiskan proses pengiriman undangan ke akun anggota dan mengaktifkan AWS Config.

Skrip secara otomatis mengaktifkan perekaman AWS Config sumber daya untuk semua sumber daya, termasuk sumber daya global, di semua Wilayah. Ini tidak membatasi pencatatan sumber daya global ke satu Wilayah. Untuk menghemat biaya, sebaiknya catat sumber daya global di satu Wilayah

saja. Jika Anda menggunakan konfigurasi pusat atau agregasi lintas wilayah, ini harus menjadi Wilayah rumah Anda. Untuk informasi selengkapnya, lihat Merekam sumber daya di AWS Config.

Ada skrip yang sesuai untuk menonaktifkan Security Hub CSPM di seluruh akun dan Wilayah.

Langkah selanjutnya: Manajemen postur dan integrasi

Setelah mengaktifkan Security Hub CSPM, sebaiknya aktifkan standar dan kontrol keamanan untuk memantau postur keamanan Anda. Setelah Anda mengaktifkan kontrol, Security Hub CSPM mulai menjalankan pemeriksaan keamanan dan menghasilkan temuan kontrol yang membantu Anda mendeteksi kesalahan konfigurasi di lingkungan Anda. AWS Untuk menerima temuan kontrol, Anda harus mengaktifkan dan mengonfigurasi AWS Config untuk Security Hub CSPM. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM.

Setelah mengaktifkan Security Hub CSPM, Anda juga dapat memanfaatkan integrasi antara Security Hub CSPM dan solusi lain Layanan AWS dan pihak ketiga untuk melihat temuan mereka di Security Hub CSPM. Security Hub CSPM mengumpulkan temuan dari sumber yang berbeda dan menelannya dalam format yang konsisten. Lihat informasi yang lebih lengkap di Memahami integrasi di Security Hub CSPM.

Mengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM

AWS Security Hub CSPM menggunakan AWS Config aturan untuk menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk sebagian besar kontrol. AWS Config memberikan tampilan rinci tentang konfigurasi AWS sumber daya di Anda Akun AWS. Ini menggunakan aturan untuk membuat konfigurasi dasar untuk sumber daya Anda dan perekam konfigurasi untuk mendeteksi apakah sumber daya tertentu melanggar ketentuan aturan.

Beberapa aturan, disebut sebagai aturan AWS Config terkelola, telah ditentukan dan dikembangkan oleh AWS Config. Aturan lainnya adalah AWS Config aturan khusus yang dikembangkan Security Hub CSPM. AWS Config aturan yang digunakan CSPM Security Hub untuk kontrol disebut sebagai aturan terkait layanan. Service-linked aturan mengizinkan Layanan AWS seperti Security Hub CSPM untuk membuat AWS Config aturan di akun Anda.

Jika Anda mengaktifkan CSPM AWS Security Hub dan Security Hub, Security Hub CSPM secara otomatis membuat perekam konfigurasi terkait layanan untuk menilai kontrol keamanan Anda. Anda tidak perlu mengaktifkan atau mengkonfigurasi secara manual AWS Config. Untuk informasi selengkapnya, lihat Menggunakan perekam konfigurasi terkait layanan.

Jika CSPM Security Hub diaktifkan tanpa Security Hub, Anda harus mengaktifkan AWS Config dan mengaktifkan perekaman sumber daya secara manual. Untuk informasi selengkapnya, lihat Mengkonfigurasi secara manual AWS Config.

AWS Config Prasyarat yang dijelaskan di halaman ini hanya berlaku untuk standar AWS keamanan, seperti Praktik Terbaik Keamanan Dasar dan Tolok AWS Ukur Yayasan CIS. AWS Standar multicloud, seperti CIS Azure Foundations Benchmark v4.0.0, tidak mengharuskan Anda untuk mengaktifkan perekaman atau mengkonfigurasi perekam konfigurasi. AWS Config Konektor multicloud Security Hub CSPM secara otomatis menyiapkan perekam terkait layanan untuk mengevaluasi sumber daya cloud eksternal. Satu-satunya prasyarat untuk standar multicloud adalah konektor CSPM Security Hub untuk penyedia cloud eksternal.

Topik

- Menggunakan perekam konfigurasi terkait layanan
- Mengkonfigurasi secara manual AWS Config
- Memahami Config.1 kontrol
- Menghasilkan aturan terkait layanan

Menggunakan perekam konfigurasi terkait layanan

Saat Anda mengaktifkan CSPM AWS Security Hub dan Security Hub, Security Hub CSPM secara otomatis membuat dan mengelola perekam konfigurasi terkait layanan di seluruh akun dan Wilayah Anda. Anda tidak perlu mengaktifkan atau mengkonfigurasi secara manual AWS Config.

Nama perekam konfigurasi ini adalah`AWSConfigurationRecorderForSecurityHubCSPM`. Security Hub CSPM membuat perekam konfigurasi terkait layanan yang sesuai untuk setiap akun dan Wilayah tempat CSPM Security Hub dan Security Hub diaktifkan. Saat Anda mengaktifkan CSPM Security Hub untuk Akun AWS s dan Wilayah AWS s baru, Security Hub CSPM secara otomatis membuat perekam konfigurasi terkait layanan.

Security Hub CSPM mengelola konfigurasi sumber daya perekam konfigurasi terkait layanan, memastikan bahwa perekaman diaktifkan untuk semua sumber daya yang terkait dengan kontrol yang didukung oleh Security Hub. Untuk daftar sumber daya yang diperlukan, lihatDiperlukanAWS Configsumber daya untuk temuan kontrol.

Saat Security Hub CSPM membuat perekam konfigurasi terkait layanan ini, Security Hub tidak menggunakan perekam konfigurasi yang dikelola pelanggan. AWS Config

Untuk informasi selengkapnya tentang perekam konfigurasi, lihat Bekerja dengan perekam konfigurasi di Panduan AWS Config Pengembang.

Mengkonfigurasi secara manual AWS Config

Langkah-langkah berikut berlaku ketika Anda mengaktifkan Security Hub CSPM tanpa Security Hub. Dalam hal ini, Anda harus mengaktifkan AWS Config akun Anda dan mengaktifkan perekaman sumber daya untuk jenis sumber daya yang dievaluasi oleh kontrol yang diaktifkan. Setelah Anda melakukan ini, Security Hub CSPM membuat AWS Config aturan yang sesuai dan mulai menjalankan pemeriksaan keamanan untuk menghasilkan temuan.

Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config

Untuk menerima temuan kontrol di Security Hub CSPM, AWS Config harus diaktifkan untuk akun Anda di setiap Wilayah AWS tempat CSPM Security Hub diaktifkan. Jika Anda menggunakan Security Hub CSPM untuk lingkungan multi-akun, AWS Config harus diaktifkan di setiap Wilayah untuk akun administrator dan semua akun anggota.

Kami sangat menyarankan agar Anda mengaktifkan perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar dan kontrol CSPM Security Hub. Ini membantu Anda memastikan bahwa temuan kontrol Anda akurat.

Untuk mengaktifkan perekaman sumber daya AWS Config, Anda harus memiliki izin yang cukup untuk merekam sumber daya dalam peran AWS Identity and Access Management (IAM) yang dilampirkan ke perekam konfigurasi. Selain itu, pastikan bahwa tidak ada kebijakan atau AWS Organizations kebijakan IAM yang AWS Config mencegah izin untuk merekam sumber daya Anda. Kontrol CSPM Security Hub mengevaluasi konfigurasi sumber daya secara langsung dan tidak memperhitungkan AWS Organizations kebijakan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat Bekerja dengan perekam konfigurasi di Panduan AWS Config Pengembang.

Jika Anda mengaktifkan standar di CSPM Security Hub tetapi belum diaktifkan AWS Config, Security Hub CSPM mencoba membuat AWS Config aturan terkait layanan sesuai dengan jadwal berikut:

- Pada hari Anda mengaktifkan standar.
- Sehari setelah Anda mengaktifkan standar.
- 3 hari setelah Anda mengaktifkan standar.
- 7 hari setelah Anda mengaktifkan standar, dan terus menerus setiap 7 hari setelahnya.

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM juga mencoba membuat AWS Config aturan terkait layanan setiap kali Anda mengaitkan kebijakan konfigurasi yang memungkinkan satu atau beberapa standar dengan akun, unit organisasi (OU), atau root.

Merekam sumber daya di AWS Config

Saat Anda mengaktifkan AWS Config, Anda harus menentukan AWS sumber daya mana yang ingin direkam oleh perekam AWS Config konfigurasi. Melalui aturan terkait layanan, perekam konfigurasi memungkinkan CSPM Security Hub mendeteksi perubahan pada konfigurasi sumber daya Anda.

Agar CSPM Security Hub menghasilkan temuan kontrol yang akurat, Anda harus mengaktifkan perekaman AWS Config untuk jenis sumber daya yang sesuai dengan kontrol yang diaktifkan. Ini terutama mengaktifkan kontrol dengan jenis jadwal yang dipicu perubahan yang memerlukan perekaman sumber daya. Beberapa kontrol dengan jenis jadwal periodik juga memerlukan perekaman sumber daya. Untuk daftar kontrol ini dan sumber daya yang sesuai, lihatDiperlukanAWS Configsumber daya untuk temuan kontrol.

⚠ Warning

Jika Anda tidak mengonfigurasi AWS Config perekaman dengan benar untuk kontrol CSPM Security Hub, ini dapat menghasilkan temuan kontrol yang tidak akurat, terutama dalam kasus berikut:

- Anda tidak pernah merekam sumber daya untuk kontrol tertentu, atau Anda menonaktifkan perekaman sumber daya sebelum membuat jenis sumber daya tersebut. Dalam kasus ini, Anda menerima `WARNING` temuan untuk kontrol yang dipermasalahkan, meskipun Anda mungkin telah membuat sumber daya dalam lingkup kontrol setelah Anda menonaktifkan perekaman. `WARNING`Temuan ini adalah temuan default yang tidak benar-benar mengevaluasi status konfigurasi sumber daya.
- Anda menonaktifkan perekaman untuk sumber daya yang dievaluasi oleh kontrol tertentu. Dalam hal ini, Security Hub CSPM mempertahankan temuan kontrol yang dihasilkan sebelum Anda menonaktifkan perekaman, meskipun kontrol tidak mengevaluasi sumber daya baru atau yang diperbarui. Security Hub CSPM juga mengubah status kepatuhan temuan menjadi. `WARNING` Temuan yang dipertahankan ini mungkin tidak secara akurat mencerminkan status konfigurasi sumber daya saat ini.

Secara default, AWS Config mencatat semua sumber daya Regional yang didukung yang ditemukan Wilayah AWS di mana ia berjalan. Untuk menerima semua temuan kontrol CSPM Security Hub, Anda

juga harus mengonfigurasi AWS Config untuk merekam sumber daya global. Untuk menghemat biaya, kami sarankan untuk mencatat sumber daya global hanya dalam satu Wilayah. Jika Anda menggunakan konfigurasi pusat atau agregasi lintas wilayah, Wilayah ini harus menjadi Wilayah asal Anda.

Di AWS Config, Anda dapat memilih antara perekaman berkelanjutan dan perekaman harian perubahan status sumber daya. Jika Anda memilih perekaman harian, AWS Config mengirimkan data konfigurasi sumber daya pada akhir setiap periode 24 jam jika ada perubahan status sumber daya. Jika tidak ada perubahan, tidak ada data yang dikirimkan. Hal ini dapat menunda pembuatan temuan CSPM Security Hub untuk kontrol yang dipicu perubahan hingga periode 24 jam selesai.

Untuk informasi selengkapnya tentang AWS Config perekaman, lihat Merekam AWS sumber daya di Panduan AWS Config Pengembang.

Cara untuk mengaktifkan dan mengkonfigurasi AWS Config

Anda dapat mengaktifkan AWS Config dan mengaktifkan perekaman sumber daya dengan salah satu cara berikut:

- AWS Config konsol — Anda dapat mengaktifkan AWS Config akun dengan menggunakan AWS Config konsol. Untuk petunjuk, lihat Menyiapkan AWS Config dengan konsol di Panduan AWS Config Pengembang.
- AWS CLI atau SDK — Anda dapat mengaktifkan AWS Config akun dengan menggunakan AWS Command Line Interface (AWS CLI). Untuk petunjuk, lihat Menyiapkan AWS Config dengan AWS CLI di Panduan AWS Config Pengembang. AWS Software Development Kit (SDK) juga tersedia untuk banyak bahasa pemrograman.
- CloudFormation template — AWS Config Untuk mengaktifkan banyak akun, kami sarankan menggunakan AWS CloudFormation template bernama Enable AWS Config. Untuk mengakses template ini, lihat AWS CloudFormation StackSet contoh template di Panduan AWS CloudFormation Pengguna.

  Secara default, template ini tidak termasuk rekaman untuk sumber daya global IAM. Pastikan Anda mengaktifkan perekaman untuk sumber daya global IAM hanya dalam satu Wilayah AWS untuk menghemat biaya perekaman. Jika Anda mengaktifkan agregasi lintas wilayah, ini harus menjadi Wilayah asal CSPM Security Hub Anda. Jika tidak, dapat berupa Wilayah mana pun yang tersedia CSPM Security Hub yang mendukung perekaman sumber daya global IAM. Kami merekomendasikan menjalankan satu StackSet untuk merekam semua sumber daya, termasuk sumber daya global IAM, di Wilayah asal atau Wilayah terpilih lainnya. Kemudian, jalankan satu

detik StackSet untuk merekam semua sumber daya kecuali sumber daya global IAM di Wilayah lain.

- GitHub script — Security Hub CSPM menawarkan GitHubskrip yang memungkinkan Security Hub CSPM dan AWS Config untuk beberapa akun di seluruh Wilayah. Skrip ini berguna jika Anda belum terintegrasi AWS Organizations, atau Anda memiliki beberapa akun anggota yang bukan bagian dari organisasi.

Untuk informasi selengkapnya, lihat posting blog berikut di blog AWS Keamanan: Optimalkan AWS Config untuk AWS Security Hub CSPM untuk mengelola postur keamanan cloud Anda secara efektif.

Pertimbangan Biaya

Security Hub CSPM dapat memengaruhi biaya perekam AWS Config konfigurasi Anda dengan memperbarui item `AWS::Config::ResourceCompliance` konfigurasi. Pembaruan dapat terjadi setiap kali kontrol CSPM Security Hub yang terkait dengan AWS Config aturan mengubah status kepatuhan, diaktifkan atau dinonaktifkan, atau memiliki pembaruan parameter. Jika Anda menggunakan perekam AWS Config konfigurasi hanya untuk Security Hub CSPM, dan tidak menggunakan item konfigurasi ini untuk tujuan lain, kami sarankan untuk mematikan perekaman untuk itu. AWS Config Ini dapat mengurangi AWS Config biaya Anda. Anda tidak perlu merekam pemeriksaan keamanan `AWS::Config::ResourceCompliance` agar berfungsi di Security Hub CSPM.

Untuk informasi tentang biaya yang terkait dengan pencatatan sumber daya, lihat harga dan AWS Config harga CSPM AWS Security Hub.

Memahami Config.1 kontrol

> **Note**
>
> Ketika AWS Security Hub CSPM dan Security Hub keduanya diaktifkan, Config.1 kontrol selalu memiliki status. `PASSED` Security Hub CSPM memiliki akses langsung ke item konfigurasi melalui perekam konfigurasi terkait layanan. Untuk informasi selengkapnya, lihat Menggunakan perekam konfigurasi terkait layanan.

Di Security Hub CSPM, Config.1kontrol menghasilkan `FAILED` temuan di akun Anda jika AWS Config dinonaktifkan. Ini juga menghasilkan `FAILED` temuan di akun Anda jika AWS Config diaktifkan tetapi perekaman sumber daya tidak diaktifkan.

Jika AWS Config diaktifkan dan perekaman sumber daya diaktifkan, tetapi perekaman sumber daya tidak diaktifkan untuk jenis sumber daya yang diperiksa oleh kontrol yang diaktifkan, Security Hub CSPM akan menghasilkan `FAILED` temuan untuk kontrol. Config.1 Selain `FAILED` temuan ini, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol yang diaktifkan dan jenis sumber daya yang diperiksa kontrol. Misalnya, jika Anda mengaktifkan KMS.5kontrol dan perekaman sumber daya tidak diaktifkan AWS KMS keys, Security Hub CSPM akan menghasilkan `FAILED` temuan untuk kontrol. Config.1 Security Hub CSPM juga menghasilkan `WARNING` temuan untuk KMS.5 kontrol dan kunci KMS Anda.

Untuk menerima `PASSED` temuan untuk Config.1 kontrol, aktifkan perekaman sumber daya untuk semua jenis sumber daya yang sesuai dengan kontrol yang diaktifkan. Juga nonaktifkan kontrol yang tidak diperlukan untuk organisasi Anda. Ini membantu memastikan bahwa Anda tidak memiliki celah konfigurasi dalam pemeriksaan kontrol keamanan Anda. Ini juga membantu memastikan bahwa Anda menerima temuan akurat tentang sumber daya yang salah konfigurasi.

Jika Anda adalah administrator CSPM Security Hub yang didelegasikan untuk organisasi, AWS Config rekaman harus dikonfigurasi dengan benar untuk akun dan akun anggota Anda. Jika Anda menggunakan agregasi lintas wilayah, AWS Config perekaman harus dikonfigurasi dengan benar di Wilayah beranda dan semua Wilayah yang ditautkan. Sumber daya global tidak perlu dicatat di Wilayah terkait.

Menghasilkan aturan terkait layanan

Untuk setiap kontrol yang menggunakan AWS Config aturan terkait layanan, Security Hub CSPM membuat instance aturan yang diperlukan di lingkungan Anda. AWS

Aturan terkait layanan ini khusus untuk Security Hub CSPM. Security Hub CSPM membuat aturan terkait layanan ini meskipun contoh lain dari aturan yang sama sudah ada. Aturan terkait layanan ditambahkan `securityhub` sebelum nama aturan asli dan pengidentifikasi unik setelah nama aturan. Misalnya, untuk aturan AWS Config terkelolavpc-flow-logs-enabled, nama aturan terkait layanan mungkin. `securityhub-vpc-flow-logs-enabled-12345`

Ada kuota untuk jumlah aturan AWS Config terkelola yang dapat digunakan untuk mengevaluasi kontrol. AWS Config aturan yang dibuat oleh Security Hub CSPM tidak diperhitungkan dalam kuota tersebut. Anda dapat mengaktifkan standar keamanan meskipun Anda telah mencapai AWS Config kuota untuk aturan terkelola di akun Anda. Untuk mempelajari kuota AWS Config aturan selengkapnya, lihat Batas layanan AWS Config di Panduan AWS Config Pengembang.

> **Note**
>
> Jika Anda menggunakan Security Hub CSPM dan Security Hub, Anda dapat melihat aturan terkait layanan AWS Config tetapi Anda tidak akan dapat melihat sumber daya yang sesuai atau tidak sesuai yang terkait dengan aturan tersebut. Sumber daya yang sesuai dan tidak sesuai hanya akan terlihat di Security Hub CSPM dan Security Hub.

Memahami konfigurasi lokal di Security Hub CSPM

Konfigurasi lokal adalah cara default AWS organisasi dikonfigurasi di Security Hub CSPM. Jika Anda tidak ikut serta dan mengaktifkan konfigurasi pusat, organisasi Anda menggunakan konfigurasi lokal secara default.

Di bawah konfigurasi lokal, akun administrator CSPM Security Hub yang didelegasikan memiliki kontrol terbatas atas pengaturan konfigurasi. Satu-satunya pengaturan yang dapat diterapkan oleh administrator yang didelegasikan secara otomatis mengaktifkan CSPM Security Hub dan standar keamanan default di akun organisasi baru. Pengaturan ini hanya berlaku di Wilayah tempat Anda menetapkan akun administrator yang didelegasikan. Standar keamanan default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Setelan konfigurasi lokal tidak berlaku untuk akun organisasi yang ada atau ke Wilayah selain yang ditunjuk untuk akun administrator yang didelegasikan.

Selain mengaktifkan CSPM Security Hub dan standar default di akun organisasi baru di satu Wilayah, Anda harus mengonfigurasi setelan CSPM Security Hub lainnya, termasuk standar dan kontrol, secara terpisah di setiap Wilayah dan akun. Karena ini bisa menjadi proses duplikatif, sebaiknya gunakan konfigurasi pusat untuk lingkungan multi-akun jika satu atau beberapa hal berikut berlaku untuk Anda:

- Anda menginginkan pengaturan konfigurasi yang berbeda untuk berbagai bagian organisasi Anda (misalnya, standar atau kontrol yang diaktifkan berbeda untuk tim yang berbeda).
- Anda beroperasi di beberapa Wilayah dan ingin mengurangi waktu dan kompleksitas mengonfigurasi layanan di seluruh Wilayah ini.
- Anda ingin akun baru menggunakan pengaturan konfigurasi tertentu saat mereka bergabung dengan organisasi.
- Anda ingin akun organisasi mewarisi pengaturan konfigurasi tertentu dari akun induk atau root.

Untuk informasi tentang konfigurasi pusat, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Memahami konfigurasi pusat di Security Hub CSPM

Konfigurasi pusat adalah fitur CSPM AWS Security Hub yang membantu Anda mengatur dan mengelola CSPM Security Hub di beberapa dan. Akun AWS Wilayah AWS Untuk menggunakan konfigurasi pusat, Anda harus terlebih dahulu mengintegrasikan Security Hub CSPM dan. AWS Organizations Anda dapat mengintegrasikan layanan dengan membuat organisasi dan menunjuk akun administrator CSPM Security Hub yang didelegasikan untuk organisasi.

Dari akun administrator CSPM Security Hub yang didelegasikan, Anda dapat mengaktifkan CSPM Security Hub untuk akun organisasi dan unit organisasi (OU) di seluruh Wilayah. Anda juga dapat mengaktifkan, mengonfigurasi, dan menonaktifkan standar keamanan individual dan kontrol keamanan untuk akun dan OU di seluruh Wilayah. Anda dapat mengonfigurasi pengaturan ini hanya dalam beberapa langkah dari satu Wilayah utama, yang disebut sebagai Wilayah asal.

Saat Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat memilih akun dan OU mana yang akan dikonfigurasi. Jika administrator yang didelegasikan menetapkan akun anggota atau OU sebagai dikelola sendiri, anggota dapat mengonfigurasi pengaturannya sendiri secara terpisah di setiap Wilayah. Jika administrator yang didelegasikan menetapkan akun anggota atau OU sebagai dikelola secara terpusat, hanya administrator yang didelegasikan yang dapat mengonfigurasi akun anggota atau OU di seluruh Wilayah. Anda dapat menetapkan semua akun dan OU di organisasi Anda sebagai dikelola secara terpusat, semua dikelola sendiri, atau kombinasi keduanya.

Untuk mengonfigurasi akun yang dikelola secara terpusat, administrator yang didelegasikan menggunakan kebijakan konfigurasi CSPM Security Hub. Kebijakan konfigurasi memungkinkan administrator yang didelegasikan menentukan apakah CSPM Security Hub diaktifkan atau dinonaktifkan, dan standar serta kontrol mana yang diaktifkan atau dinonaktifkan. Mereka juga dapat digunakan untuk menyesuaikan parameter untuk kontrol tertentu.

Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan. Administrator yang didelegasikan menentukan Wilayah asal organisasi dan Wilayah yang ditautkan sebelum mulai menggunakan konfigurasi pusat. Menentukan Wilayah terkait adalah opsional. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi tunggal untuk seluruh organisasi, atau membuat beberapa kebijakan konfigurasi untuk mengonfigurasi setelan variabel untuk akun dan OU yang berbeda.

> **Tip**
>
> Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengonfigurasi CSPM Security Hub secara terpisah di setiap akun dan Wilayah. Ini disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan dapat secara otomatis mengaktifkan CSPM Security Hub dan serangkaian standar keamanan terbatas di akun organisasi baru di Wilayah saat ini. Konfigurasi lokal tidak berlaku untuk akun organisasi yang ada atau Wilayah selain Wilayah saat ini. Konfigurasi lokal juga tidak mendukung penggunaan kebijakan konfigurasi.

Bagian ini memberikan gambaran umum tentang konfigurasi pusat.

Manfaat menggunakan konfigurasi pusat

Manfaat konfigurasi pusat meliputi:

Menyederhanakan konfigurasi layanan dan kemampuan CSPM Security Hub

Bila Anda menggunakan konfigurasi pusat, Security Hub CSPM memandu Anda melalui proses mengonfigurasi praktik terbaik keamanan untuk organisasi Anda. Ini juga menerapkan kebijakan konfigurasi yang dihasilkan ke akun tertentu dan OU secara otomatis. Jika Anda memiliki setelan CSPM Security Hub yang ada, seperti mengaktifkan kontrol keamanan baru secara otomatis, Anda dapat menggunakannya sebagai titik awal untuk kebijakan konfigurasi Anda. Selain itu, halaman Konfigurasi di konsol CSPM Security Hub menampilkan ringkasan real-time dari kebijakan konfigurasi Anda dan akun dan OU mana yang menggunakan setiap kebijakan.

Konfigurasikan di seluruh akun dan Wilayah

Anda dapat menggunakan konfigurasi pusat untuk mengonfigurasi CSPM Security Hub di beberapa akun dan Wilayah. Ini membantu memastikan bahwa setiap bagian dari organisasi Anda mempertahankan konfigurasi yang konsisten dan cakupan keamanan yang memadai.

Mengakomodasi konfigurasi yang berbeda di akun dan OU yang berbeda

Dengan konfigurasi pusat, Anda dapat memilih untuk mengonfigurasi akun dan OU organisasi Anda dengan berbagai cara. Misalnya, akun pengujian dan akun produksi Anda mungkin memerlukan konfigurasi yang berbeda. Anda juga dapat membuat kebijakan konfigurasi yang mencakup akun baru saat mereka bergabung dengan organisasi.

Mencegah penyimpangan konfigurasi

Drift konfigurasi terjadi ketika pengguna membuat perubahan pada layanan atau fitur yang bertentangan dengan pilihan administrator yang didelegasikan. Konfigurasi pusat mencegah penyimpangan ini. Saat Anda menetapkan akun atau OU sebagai dikelola secara terpusat, akun tersebut hanya dapat dikonfigurasi oleh administrator yang didelegasikan untuk organisasi. Jika Anda lebih suka akun tertentu atau OU untuk mengonfigurasi pengaturannya sendiri, Anda dapat menetapkannya sebagai dikelola sendiri.

Kapan menggunakan konfigurasi pusat?

Konfigurasi pusat paling bermanfaat untuk AWS lingkungan yang mencakup beberapa akun CSPM Security Hub. Ini dirancang untuk membantu Anda mengelola CSPM Security Hub secara terpusat untuk beberapa akun.

Anda dapat menggunakan konfigurasi pusat untuk mengonfigurasi layanan CSPM Security Hub, standar keamanan, dan kontrol keamanan. Anda juga dapat menggunakannya untuk menyesuaikan parameter kontrol tertentu. Untuk informasi selengkapnya tentang standar keamanan, lihatMemahami standar keamanan di Security Hub CSPM. Untuk informasi selengkapnya tentang kontrol keamanan, lihatMemahami kontrol keamanan di Security Hub CSPM.

Istilah dan konsep konfigurasi pusat

Memahami istilah dan konsep utama berikut dapat membantu Anda menggunakan konfigurasi pusat CSPM Security Hub.

Konfigurasi pusat

Fitur CSPM Security Hub yang membantu akun administrator CSPM Security Hub yang didelegasikan untuk organisasi mengonfigurasi layanan CSPM Security Hub, standar keamanan, dan kontrol keamanan di beberapa akun dan Wilayah. Untuk mengonfigurasi setelan ini, administrator yang didelegasikan membuat dan mengelola kebijakan konfigurasi CSPM Security Hub untuk akun yang dikelola secara terpusat di organisasinya. Self-managed akun dapat mengonfigurasi pengaturan mereka sendiri secara terpisah di setiap Wilayah. Untuk menggunakan konfigurasi pusat, Anda harus mengintegrasikan Security Hub CSPM dan. AWS Organizations

Beranda Wilayah

Wilayah AWS Dari mana administrator yang didelegasikan secara terpusat mengonfigurasi CSPM Security Hub, dengan membuat dan mengelola kebijakan konfigurasi. Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan.

Wilayah asal juga berfungsi sebagai Wilayah agregasi CSPM Security Hub, menerima temuan, wawasan, dan data lainnya dari Wilayah terkait.

Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah keikutsertaan. Wilayah keikutsertaan tidak bisa menjadi Wilayah asal, tetapi bisa menjadi Wilayah terkait. Untuk daftar Wilayah keikutsertaan, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi Manajemen Akun.AWS

Wilayah Tertaut

An Wilayah AWS yang dapat dikonfigurasi dari Wilayah asal. Kebijakan konfigurasi dibuat oleh administrator yang didelegasikan di Wilayah beranda. Kebijakan berlaku di Wilayah asal dan semua Wilayah terkait. Menentukan Wilayah terkait adalah opsional.

Wilayah terkait juga mengirimkan temuan, wawasan, dan data lainnya ke Wilayah asal.

Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah keikutsertaan. Anda harus mengaktifkan Wilayah tersebut untuk akun sebelum kebijakan konfigurasi dapat diterapkan padanya. Akun manajemen Organisasi dapat mengaktifkan Wilayah keikutsertaan untuk akun anggota. Untuk informasi selengkapnya, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan Referensi Manajemen AWS Akun.

Target

Sebuah Akun AWS, unit organisasi (OU), atau akar organisasi.

Kebijakan konfigurasi CSPM Security Hub

Kumpulan setelan CSPM Security Hub yang dapat dikonfigurasi oleh administrator yang didelegasikan untuk target yang dikelola secara terpusat. Hal ini mencakup:

- Apakah akan mengaktifkan atau menonaktifkan Security Hub CSPM.
- Apakah akan mengaktifkan satu atau lebih standar keamanan.
- Kontrol keamanan mana yang diaktifkan di seluruh standar yang diaktifkan. Administrator yang didelegasikan dapat melakukan ini dengan menyediakan daftar kontrol khusus yang harus diaktifkan, dan Security Hub CSPM menonaktifkan semua kontrol lainnya (termasuk kontrol baru saat dirilis). Atau, administrator yang didelegasikan dapat memberikan daftar kontrol

khusus yang harus dinonaktifkan, dan Security Hub CSPM mengaktifkan semua kontrol lainnya (termasuk kontrol baru saat dirilis).

- Secara opsional, sesuaikan parameter untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah tertaut setelah dikaitkan dengan setidaknya satu akun, unit organisasi (OU), atau root.

Pada konsol CSPM Security Hub, administrator yang didelegasikan dapat memilih kebijakan konfigurasi yang direkomendasikan CSPM Security Hub atau membuat kebijakan konfigurasi khusus. Dengan Security Hub CSPM API dan AWS CLI, administrator yang didelegasikan hanya dapat membuat kebijakan konfigurasi kustom. Administrator yang didelegasikan dapat membuat maksimal 20 kebijakan konfigurasi kustom.

Dalam kebijakan konfigurasi yang direkomendasikan, Security Hub CSPM, standar AWS Foundational Security Best Practices (FSBP), dan semua kontrol FSBP yang ada dan yang baru diaktifkan. Kontrol yang menerima parameter menggunakan nilai default. Kebijakan konfigurasi yang disarankan berlaku untuk seluruh organisasi.

Untuk menerapkan setelan berbeda ke organisasi, atau menerapkan kebijakan konfigurasi yang berbeda ke akun dan OU yang berbeda, buat kebijakan konfigurasi khusus.

> **Note**
>
> Kebijakan konfigurasi hanya mendukung standar dan kontrol AWS keamanan. Standar multicloud, seperti CIS Azure Foundations Benchmark v4.0.0, dan kontrol multicloud terkait tidak dapat dimasukkan dalam kebijakan konfigurasi. Untuk mengaktifkan atau mengkonfigurasi standar multicloud, gunakan mekanisme konfigurasi lokal langsung di yang diinginkan. Akun AWS

Konfigurasi lokal

Jenis konfigurasi default untuk organisasi, setelah mengintegrasikan Security Hub CSPM dan. AWS Organizations Dengan konfigurasi lokal, administrator yang didelegasikan dapat memilih untuk mengaktifkan CSPM Security Hub secara otomatis dan standar keamanan default di akun organisasi baru di Wilayah saat ini. Jika administrator yang didelegasikan secara otomatis mengaktifkan standar default, semua kontrol yang merupakan bagian dari standar ini juga diaktifkan secara otomatis dengan parameter default untuk akun organisasi baru. Pengaturan

ini tidak berlaku untuk akun yang ada, jadi penyimpangan konfigurasi dimungkinkan setelah akun bergabung dengan organisasi. Menonaktifkan kontrol spesifik yang merupakan bagian dari standar default, dan mengonfigurasi standar dan kontrol tambahan, harus dilakukan secara terpisah di setiap akun dan Wilayah.

Konfigurasi lokal tidak mendukung penggunaan kebijakan konfigurasi. Untuk menggunakan kebijakan konfigurasi, Anda harus beralih ke konfigurasi pusat.

Manajemen akun manual

Jika Anda tidak mengintegrasikan CSPM Security Hub dengan AWS Organizations atau memiliki akun mandiri, Anda harus menentukan pengaturan untuk setiap akun secara terpisah di setiap Wilayah. Manajemen akun manual tidak mendukung penggunaan kebijakan konfigurasi.

API konfigurasi pusat

Operasi CSPM Security Hub yang hanya administrator CSPM Security Hub yang didelegasikan CSPM Security Hub yang dapat digunakan di Wilayah asal untuk mengelola kebijakan konfigurasi untuk akun yang dikelola secara terpusat. Operasi meliputi:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

Account-specific API

Operasi CSPM Security Hub yang dapat digunakan untuk mengaktifkan atau menonaktifkan Security Hub CSPM, standar, dan kontrol berdasarkan akun per akun. Operasi ini digunakan di masing-masing Wilayah.

Self-managed akun dapat menggunakan operasi khusus akun untuk mengonfigurasi pengaturan mereka sendiri. Akun yang dikelola secara terpusat tidak dapat menggunakan operasi khusus akun berikut di Wilayah asal dan Wilayah yang ditautkan. Di Wilayah tersebut, hanya

administrator yang didelegasikan yang dapat mengonfigurasi akun yang dikelola secara terpusat melalui operasi konfigurasi pusat dan kebijakan konfigurasi.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Untuk memeriksa status akun, pemilik akun yang dikelola secara terpusat dapat menggunakan salah satu `Get` atau `Describe` operasi Security Hub CSPM API.

Jika Anda menggunakan konfigurasi lokal atau manajemen akun manual, alih-alih konfigurasi pusat, operasi khusus akun ini dapat digunakan.

Self-managed Akun juga dapat digunakan `*Invitations` dan `*Members` beroperasi. Namun, kami menyarankan agar akun yang dikelola sendiri tidak menggunakan operasi ini. Asosiasi kebijakan dapat gagal jika akun anggota memiliki anggotanya sendiri yang merupakan bagian dari organisasi yang berbeda dari administrator yang didelegasikan.

Unit organisasi (OU)

Di AWS Organizations dan Security Hub CSPM, wadah untuk sekelompok. Akun AWS Unit organisasi (OU) juga dapat berisi OU lain, memungkinkan Anda untuk membuat hierarki yang menyerupai pohon terbalik, dengan OU induk di bagian atas dan cabang OU yang menjangkau ke bawah, berakhir dengan akun yang merupakan daun pohon. OU dapat memiliki tepat satu orang tua, dan setiap akun organisasi dapat menjadi anggota dari satu OU.

Anda dapat mengelola OU di AWS Organizations atau AWS Control Tower. Untuk informasi selengkapnya, lihat Mengelola unit organisasi dalam Panduan AWS Organizations Pengguna atau Mengatur organisasi dan akun AWS Control Tower di Panduan AWS Control Tower Pengguna.

Administrator yang didelegasikan dapat mengaitkan kebijakan konfigurasi dengan akun atau OU tertentu, atau dengan root untuk mencakup semua akun dan OU dalam suatu organisasi.

Dikelola secara terpusat

Target yang hanya dapat dikonfigurasi oleh administrator yang didelegasikan di seluruh Wilayah dengan menggunakan kebijakan konfigurasi.

Akun administrator yang didelegasikan menentukan apakah target dikelola secara terpusat. Administrator yang didelegasikan juga dapat mengubah status target dari yang dikelola secara terpusat menjadi dikelola sendiri, atau sebaliknya.

Self-managed

Target yang mengelola pengaturan CSPM Security Hub sendiri. Target yang dikelola sendiri menggunakan operasi khusus akun untuk mengonfigurasi CSPM Security Hub untuk dirinya sendiri secara terpisah di setiap Wilayah. Ini berbeda dengan target yang dikelola secara terpusat, yang hanya dapat dikonfigurasi oleh administrator yang didelegasikan di seluruh Wilayah melalui kebijakan konfigurasi.

Akun administrator yang didelegasikan menentukan apakah target dikelola sendiri. Administrator yang didelegasikan dapat menerapkan perilaku yang dikelola sendiri ke target. Atau, akun atau OU dapat mewarisi perilaku yang dikelola sendiri dari orang tua.

Akun administrator yang didelegasikan itu sendiri dapat menjadi akun yang dikelola sendiri. Akun administrator yang didelegasikan dapat mengubah status target dari dikelola sendiri menjadi dikelola secara terpusat, atau sebaliknya.

Asosiasi kebijakan konfigurasi

Tautan antara kebijakan konfigurasi dan akun, unit organisasi (OU), atau root. Ketika asosiasi kebijakan ada, akun, OU, atau root menggunakan pengaturan yang ditentukan oleh kebijakan konfigurasi. Asosiasi ada dalam salah satu dari kasus ini:

- Ketika administrator yang didelegasikan secara langsung menerapkan kebijakan konfigurasi ke akun, OU, atau root
- Ketika akun atau OU mewarisi kebijakan konfigurasi dari OU induk atau root

Asosiasi ada sampai konfigurasi yang berbeda diterapkan atau diwariskan.

Kebijakan konfigurasi yang diterapkan

Jenis asosiasi kebijakan konfigurasi di mana administrator yang didelegasikan secara langsung menerapkan kebijakan konfigurasi ke akun target, OU, atau root. Target dikonfigurasi dengan cara yang ditentukan oleh kebijakan konfigurasi, dan hanya administrator yang didelegasikan yang dapat mengubah konfigurasinya. Jika diterapkan ke root, kebijakan konfigurasi memengaruhi semua akun dan OU di organisasi yang tidak menggunakan konfigurasi berbeda melalui aplikasi atau warisan dari induk terdekat.

Administrator yang didelegasikan juga dapat menerapkan konfigurasi yang dikelola sendiri ke akun tertentu, OU, atau root.

Kebijakan konfigurasi yang diwariskan

Jenis asosiasi kebijakan konfigurasi di mana akun atau OU mengadopsi konfigurasi OU induk terdekat atau root. Jika kebijakan konfigurasi tidak langsung diterapkan ke akun atau OU, kebijakan tersebut mewarisi konfigurasi induk terdekat. Semua elemen kebijakan diwariskan. Dengan kata lain, akun atau OU tidak dapat memilih untuk secara selektif mewarisi hanya bagian dari kebijakan. Jika orang tua terdekat dikelola sendiri, akun anak atau OU mewarisi perilaku yang dikelola sendiri dari orang tua.

Warisan tidak dapat mengganti konfigurasi yang diterapkan. Artinya, jika kebijakan konfigurasi atau konfigurasi yang dikelola sendiri langsung diterapkan ke akun atau OU, ia menggunakan konfigurasi itu dan tidak mewarisi konfigurasi induk.

Akar

Dalam AWS Organizations dan Security Hub CSPM, node induk tingkat atas dalam suatu organisasi. Jika administrator yang didelegasikan menerapkan kebijakan konfigurasi ke root, kebijakan tersebut dikaitkan dengan semua akun dan OU di organisasi kecuali mereka menggunakan kebijakan yang berbeda, melalui aplikasi atau warisan, atau ditetapkan sebagai dikelola sendiri. Jika administrator menetapkan root sebagai dikelola sendiri, semua akun dan OU dalam organisasi dikelola sendiri kecuali mereka menggunakan kebijakan konfigurasi melalui aplikasi atau warisan. Jika root dikelola sendiri dan tidak ada kebijakan konfigurasi saat ini, semua akun baru di organisasi akan mempertahankan pengaturannya saat ini.

Akun baru yang bergabung dengan organisasi berada di bawah root sampai mereka ditugaskan ke OU tertentu. Jika akun baru tidak ditetapkan ke OU, akun tersebut mewarisi konfigurasi root kecuali administrator yang didelegasikan menetapkannya sebagai akun yang dikelola sendiri.

Mengaktifkan konfigurasi pusat di Security Hub CSPM

Akun administrator CSPM AWS Security Hub yang didelegasikan dapat menggunakan konfigurasi pusat untuk mengonfigurasi CSPM, standar, dan kontrol Security Hub untuk beberapa akun dan unit organisasi (OU) secara keseluruhan. Wilayah AWS

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Bagian ini menjelaskan prasyarat untuk konfigurasi pusat dan cara mulai menggunakannya.

Prasyarat untuk konfigurasi pusat

Sebelum Anda dapat mulai menggunakan konfigurasi pusat, Anda harus mengintegrasikan Security Hub CSPM dengan AWS Organizations dan menunjuk Wilayah rumah. Jika Anda menggunakan konsol CSPM Security Hub, prasyarat ini disertakan dalam alur kerja opt-in untuk konfigurasi pusat.

Integrasi dengan Organizations

Anda harus mengintegrasikan Security Hub CSPM dan Organizations untuk menggunakan konfigurasi pusat.

Untuk mengintegrasikan layanan ini, Anda mulai dengan membuat organisasi di Organizations. Dari akun manajemen Organizations, Anda kemudian menunjuk akun administrator yang didelegasikan CSPM Security Hub. Untuk petunjuk, lihat Mengintegrasikan CSPM Security Hub denganAWS Organizations.

Pastikan bahwa Anda menunjuk administrator yang didelegasikan di Wilayah rumah yang dituju. Saat Anda mulai menggunakan konfigurasi pusat, administrator yang didelegasikan yang sama secara otomatis diatur di semua Wilayah yang ditautkan juga. Akun manajemen Organisasi tidak dapat ditetapkan sebagai akun administrator yang didelegasikan.

> **Important**
>
> Bila Anda menggunakan konfigurasi pusat, Anda tidak dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API untuk mengubah atau menghapus akun administrator yang didelegasikan. Jika akun manajemen Organizations menggunakan AWS Organizations API untuk mengubah atau menghapus administrator delegasi CSPM Security Hub, CSPM Security Hub secara otomatis menghentikan konfigurasi pusat. Kebijakan konfigurasi Anda juga dipisahkan dan dihapus. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus.

Tentukan Wilayah rumah

Anda harus menunjuk Wilayah rumah untuk menggunakan konfigurasi pusat. Wilayah asal adalah Wilayah tempat administrator yang didelegasikan mengkonfigurasi organisasi.

> **Note**
>
> Wilayah asal tidak dapat menjadi Wilayah yang AWS telah ditetapkan sebagai Wilayah keikutsertaan. Wilayah keikutsertaan dinonaktifkan secara default. Untuk daftar Wilayah keikutsertaan, lihat Pertimbangan sebelum mengaktifkan dan menonaktifkan Wilayah di Panduan Referensi Manajemen Akun. AWS

Secara opsional, Anda dapat menentukan satu atau beberapa Wilayah tertaut yang dapat dikonfigurasi dari Wilayah beranda.

Administrator yang didelegasikan dapat membuat dan mengelola kebijakan konfigurasi hanya dari Wilayah beranda. Kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang hanya berlaku untuk subset Wilayah ini, dan bukan yang lain. Pengecualian untuk ini adalah kontrol yang melibatkan sumber daya global. Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Untuk informasi selengkapnya, lihat Kontrol yang menggunakan sumber daya global.

Wilayah asal juga merupakan Wilayah agregasi CSPM Security Hub Anda yang menerima temuan, wawasan, dan data lainnya dari Wilayah tertaut.

Jika Anda telah menetapkan Region agregasi untuk agregasi Cross-region, maka itu adalah Region home default Anda untuk konfigurasi pusat. Anda dapat mengubah Wilayah rumah sebelum mulai menggunakan konfigurasi pusat dengan menghapus agregator temuan Anda saat ini dan membuat yang baru di Wilayah rumah yang Anda inginkan. Agregator temuan adalah sumber daya CSPM Security Hub yang menentukan Wilayah asal dan Wilayah terkait.

Untuk menunjuk Wilayah asal, lihat langkah-langkah untuk menyetel Wilayah agregasi. Jika Anda sudah memiliki Wilayah beranda, Anda dapat memanggil GetFindingAggregatorAPI untuk melihat detailnya, termasuk Wilayah mana yang saat ini ditautkan dengannya.

Petunjuk untuk mengaktifkan konfigurasi pusat

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan konfigurasi pusat untuk organisasi Anda.

Security Hub CSPM console

Untuk mengaktifkan konfigurasi pusat (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, pilih Pengaturan dan Konfigurasi. Kemudian, pilih Mulai konfigurasi pusat.

   Jika Anda melakukan onboarding ke Security Hub CSPM, pilih Buka CSPM Security Hub.
3. Pada halaman Tentukan administrator yang didelegasikan, pilih akun administrator yang didelegasikan atau masukkan ID akunnya. Jika berlaku, sebaiknya pilih administrator yang didelegasikan sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya. Pilih Setel administrator yang didelegasikan.
4. Pada halaman Sentralisasi organisasi, di bagian Wilayah, pilih Wilayah rumah Anda. Anda harus masuk ke Wilayah asal untuk melanjutkan. Jika Anda telah menetapkan Region agregasi untuk agregasi Cross-region, itu akan ditampilkan sebagai Region beranda. Untuk mengubah wilayah beranda, pilih Edit pengaturan Wilayah. Anda kemudian dapat memilih Wilayah rumah pilihan Anda dan kembali ke alur kerja ini.
5. Pilih setidaknya satu Wilayah untuk ditautkan ke Wilayah asal. Secara opsional, pilih apakah Anda ingin secara otomatis menautkan Wilayah yang didukung future ke Wilayah asal. Wilayah yang Anda pilih di sini akan dapat dikonfigurasi dari Wilayah asal oleh administrator yang didelegasikan. Kebijakan konfigurasi berlaku di Wilayah asal Anda dan semua Wilayah yang ditautkan.
6. Pilih Konfirmasi dan lanjutkan.
7. Anda sekarang dapat menggunakan konfigurasi pusat. Lanjutkan mengikuti petunjuk konsol untuk membuat kebijakan konfigurasi pertama Anda. Jika Anda belum siap untuk membuat kebijakan konfigurasi, pilih Saya belum siap untuk mengonfigurasi. Anda dapat membuat kebijakan nanti dengan memilih Pengaturan dan Konfigurasi di panel navigasi. Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi.

Security Hub CSPM API

Untuk mengaktifkan konfigurasi pusat (API)

1. Menggunakan kredensional akun administrator yang didelegasikan, panggil UpdateOrganizationConfigurationAPI dari Wilayah beranda.

2. Atur `AutoEnable` bidang ke`false`.
3. Atur `ConfigurationType` bidang di `OrganizationConfiguration` objek ke`CENTRAL`. Tindakan ini memiliki dampak sebagai berikut:
   - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub di semua Wilayah yang ditautkan.
   - Mengaktifkan CSPM Security Hub di akun administrator yang didelegasikan di semua Wilayah yang ditautkan.
   - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub untuk akun baru dan yang sudah ada yang menggunakan Security Hub CSPM dan milik organisasi. Ini terjadi di Wilayah asal dan semua Wilayah yang terkait. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi baru hanya jika akun tersebut dikaitkan dengan kebijakan konfigurasi yang mengaktifkan CSPM Security Hub. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi yang ada hanya jika akun tersebut sudah mengaktifkan CSPM Security Hub.
   - Setel AutoEnableke `false` semua Wilayah tertaut, dan disetel AutoEnableStandardske `NONE` Wilayah asal dan semua Wilayah yang ditautkan. Parameter ini tidak relevan di wilayah beranda dan terkait saat Anda menggunakan konfigurasi pusat, tetapi Anda dapat secara otomatis mengaktifkan CSPM Security Hub dan standar keamanan default di akun organisasi melalui penggunaan kebijakan konfigurasi.
4. Anda sekarang dapat menggunakan konfigurasi pusat. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi CSPM Security Hub di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi.

Contoh permintaan API:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

Untuk mengaktifkan konfigurasi pusat (AWS CLI)

1. Menggunakan kredensi akun administrator yang didelegasikan, jalankan update-organization-configurationperintah dari wilayah rumah.
2. Sertakan `no-auto-enable` parameternya.
3. Atur `ConfigurationType` bidang di `organization-configuration` objek ke`CENTRAL`. Tindakan ini memiliki dampak sebagai berikut:

   - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub di semua Wilayah yang ditautkan.
   - Mengaktifkan CSPM Security Hub di akun administrator yang didelegasikan di semua Wilayah yang ditautkan.
   - Menetapkan akun panggilan sebagai administrator yang didelegasikan CSPM Security Hub untuk akun baru dan yang sudah ada yang menggunakan Security Hub CSPM dan milik organisasi. Ini terjadi di Wilayah asal dan semua Wilayah yang terkait. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi baru hanya jika akun tersebut dikaitkan dengan kebijakan konfigurasi yang mengaktifkan Security Hub. Akun panggilan ditetapkan sebagai administrator yang didelegasikan untuk akun organisasi yang ada hanya jika akun tersebut sudah mengaktifkan CSPM Security Hub.
   - Menetapkan opsi pengaktifan otomatis ke no-auto-enablesemua Wilayah yang ditautkan, dan disetel auto-enable-standardske Wilayah `NONE` beranda dan semua Wilayah yang ditautkan. Parameter ini tidak relevan di wilayah beranda dan terkait saat Anda menggunakan konfigurasi pusat, tetapi Anda dapat secara otomatis mengaktifkan CSPM Security Hub dan standar keamanan default di akun organisasi melalui penggunaan kebijakan konfigurasi.
4. Anda sekarang dapat menggunakan konfigurasi pusat. Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi CSPM Security Hub di organisasi Anda. Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi.

Contoh perintah:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Target yang dikelola secara terpusat versus yang dikelola sendiri

Saat Anda mengaktifkan konfigurasi pusat, administrator CSPM AWS Security Hub yang didelegasikan dapat menetapkan setiap akun organisasi, unit organisasi (OU), dan root sebagai dikelola secara terpusat atau dikelola sendiri. Jenis manajemen target menentukan bagaimana Anda dapat menentukan pengaturan CSPM Security Hub.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Bagian ini menjelaskan perbedaan antara penunjukan yang dikelola secara terpusat dan dikelola sendiri dan bagaimana memilih jenis manajemen akun, OU, atau root.

Self-managed

Pemilik akun yang dikelola sendiri, OU, atau root harus mengonfigurasi pengaturannya secara terpisah di masing-masing Wilayah AWS akun. Administrator yang didelegasikan tidak dapat membuat kebijakan konfigurasi untuk target yang dikelola sendiri.

Dikelola secara terpusat

Hanya administrator CSPM Security Hub yang didelegasikan yang dapat mengonfigurasi pengaturan untuk akun yang dikelola secara terpusat, OU, atau root di seluruh Wilayah beranda dan Wilayah yang ditautkan. Kebijakan konfigurasi dapat dikaitkan dengan akun dan OU yang dikelola secara terpusat.

Administrator yang didelegasikan dapat mengubah status target antara dikelola sendiri dan dikelola secara terpusat. Secara default, semua akun dan OU dikelola sendiri saat Anda memulai konfigurasi pusat melalui Security Hub CSPM API. Di konsol, jenis manajemen bergantung pada kebijakan konfigurasi pertama Anda. Akun dan OU yang Anda kaitkan dengan kebijakan pertama Anda dikelola secara terpusat. Akun lain dan OU dikelola sendiri secara default.

Jika Anda mengaitkan kebijakan konfigurasi dengan akun yang dikelola sendiri sebelumnya, setelan kebijakan akan mengganti penunjukan yang dikelola sendiri. Akun menjadi dikelola secara terpusat dan mengadopsi pengaturan yang tercermin dalam kebijakan konfigurasi.

Jika Anda mengubah akun yang dikelola secara terpusat menjadi akun yang dikelola sendiri, pengaturan yang sebelumnya diterapkan ke akun melalui kebijakan konfigurasi tetap berlaku.

Misalnya, akun yang dikelola secara terpusat pada awalnya dapat dikaitkan dengan kebijakan yang mengaktifkan CSPM Security Hub, mengaktifkan Praktik Terbaik Keamanan AWS Dasar, dan dinonaktifkan. CloudTrail.1 Jika Anda kemudian menetapkan akun sebagai dikelola sendiri, semua pengaturan tetap tidak berubah. Namun, pemilik akun dapat secara mandiri mengubah pengaturan untuk akun ke depan.

Akun anak dan OU dapat mewarisi perilaku yang dikelola sendiri dari induk yang dikelola sendiri, dengan cara yang sama seperti akun anak dan OU dapat mewarisi kebijakan konfigurasi dari induk yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Asosiasi kebijakan melalui aplikasi dan warisan.

Akun yang dikelola sendiri atau OU tidak dapat mewarisi kebijakan konfigurasi dari node induk atau dari root. Misalnya, jika Anda ingin semua akun dan OU di organisasi Anda mewarisi kebijakan konfigurasi dari root, Anda harus mengubah jenis manajemen node yang dikelola sendiri menjadi dikelola secara terpusat.

Opsi untuk mengonfigurasi pengaturan di akun yang dikelola sendiri

Self-managed akun harus mengonfigurasi pengaturan mereka sendiri secara terpisah di setiap Wilayah.

Pemilik akun yang dikelola sendiri dapat menjalankan operasi API CSPM Security Hub berikut di setiap Wilayah untuk mengonfigurasi setelannya:

- `EnableSecurityHub`dan `DisableSecurityHub` untuk mengaktifkan atau menonaktifkan layanan CSPM Security Hub (jika akun yang dikelola sendiri memiliki administrator CSPM Security Hub yang didelegasikan, administrator harus memisahkan akun sebelum pemilik akun dapat menonaktifkan CSPM Security Hub).
- `BatchEnableStandards`dan `BatchDisableStandards` untuk mengaktifkan atau menonaktifkan standar
- `BatchUpdateStandardsControlAssociations`atau `UpdateStandardsControl` untuk mengaktifkan atau menonaktifkan kontrol

Self-managed Akun juga dapat digunakan `*Invitations` dan `*Members` beroperasi. Namun, kami menyarankan agar akun yang dikelola sendiri tidak menggunakan operasi ini. Asosiasi kebijakan dapat gagal jika akun anggota memiliki anggotanya sendiri yang merupakan bagian dari organisasi yang berbeda dari administrator yang didelegasikan.

Untuk deskripsi tindakan API CSPM Security Hub, lihat Referensi API CSPM AWS Security Hub.

Self-managed akun juga dapat menggunakan konsol CSPM Security Hub atau AWS CLI untuk mengonfigurasi pengaturannya di setiap Wilayah.

Self-managed akun tidak dapat menjalankan API apa pun yang terkait dengan kebijakan konfigurasi dan asosiasi kebijakan CSPM Security Hub. Hanya administrator yang didelegasikan yang dapat memanggil API konfigurasi pusat dan menggunakan kebijakan konfigurasi untuk mengonfigurasi akun yang dikelola secara terpusat.

Memilih jenis manajemen target

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menetapkan akun atau OU sebagai dikelola secara terpusat atau dikelola sendiri di AWS Security Hub CSPM.

Security Hub CSPM console

Untuk memilih jenis manajemen akun atau OU

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensional akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Pilih Konfigurasi.
3. Pada tab Organisasi, pilih akun target atau OU. Pilih Edit.
4. Pada halaman Tentukan konfigurasi, untuk tipe Manajemen, pilih Dikelola secara terpusat jika Anda ingin administrator yang didelegasikan mengonfigurasi akun target atau OU. Kemudian, pilih Terapkan kebijakan tertentu jika Anda ingin mengaitkan kebijakan konfigurasi yang ada dengan target. Pilih Mewarisi dari organisasi saya jika Anda ingin target mewarisi konfigurasi induk terdekatnya. Pilih Self-managedapakah Anda ingin akun atau OU mengonfigurasi pengaturannya sendiri.
5. Pilih Berikutnya. Tinjau perubahan Anda, dan pilih Simpan.

Security Hub CSPM API

Untuk memilih jenis manajemen akun atau OU

1. Memanggil StartConfigurationPolicyAssociationAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.
2. Untuk `ConfigurationPolicyIdentifier` bidang ini, berikan `SELF_MANAGED_SECURITY_HUB` jika Anda ingin akun atau OU mengontrol pengaturannya

sendiri. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang relevan jika Anda ingin administrator yang didelegasikan mengontrol pengaturan untuk akun atau OU.

3. Untuk `Target` bidang, berikan Akun AWS ID, ID OU, atau ID root target yang tipe manajemennya ingin Anda ubah. Ini mengaitkan perilaku yang dikelola sendiri atau kebijakan konfigurasi tertentu dengan target. Akun anak dari target dapat mewarisi kebijakan perilaku atau konfigurasi yang dikelola sendiri.

Contoh permintaan API untuk menunjuk akun yang dikelola sendiri:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Untuk memilih jenis manajemen akun atau OU

1. Jalankan start-configuration-policy-associationperintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.
2. Untuk `configuration-policy-identifier` bidang, berikan `SELF_MANAGED_SECURITY_HUB` jika Anda ingin akun atau OU mengontrol pengaturannya sendiri. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang relevan jika Anda ingin administrator yang didelegasikan untuk mengontrol pengaturan untuk akun atau OU..
3. Untuk `target` bidang, berikan Akun AWS ID, ID OU, atau ID root target yang tipe manajemennya ingin Anda ubah. Ini mengaitkan perilaku yang dikelola sendiri atau kebijakan konfigurasi tertentu dengan target. Akun anak dari target dapat mewarisi kebijakan perilaku atau konfigurasi yang dikelola sendiri.

Contoh perintah untuk menunjuk akun yang dikelola sendiri:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

Cara kerja kebijakan konfigurasi di Security Hub CSPM

Administrator CSPM AWS Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengonfigurasi CSPM Security Hub, standar keamanan, dan kontrol keamanan untuk organisasi. Setelah membuat kebijakan konfigurasi, administrator yang didelegasikan dapat mengaitkannya dengan akun tertentu, unit organisasi (OU), atau root. Kebijakan tersebut kemudian berlaku di akun tertentu, OU, atau root.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Bagian ini memberikan gambaran rinci tentang kebijakan konfigurasi.

Pertimbangan kebijakan

Sebelum Anda membuat kebijakan konfigurasi di Security Hub CSPM, pertimbangkan detail berikut.

- Kebijakan konfigurasi harus dikaitkan agar berlaku — Setelah membuat kebijakan konfigurasi, Anda dapat mengaitkannya dengan satu atau beberapa akun, unit organisasi (OU), atau root. Kebijakan konfigurasi dapat dikaitkan dengan akun atau OU melalui aplikasi langsung, atau melalui warisan dari OU induk.
- Akun atau OU hanya dapat dikaitkan dengan satu kebijakan konfigurasi — Untuk mencegah pengaturan yang bertentangan, akun atau OU hanya dapat dikaitkan dengan satu kebijakan konfigurasi pada waktu tertentu. Atau, akun atau OU dapat dikelola sendiri.
- Kebijakan konfigurasi selesai — Kebijakan konfigurasi menyediakan spesifikasi pengaturan yang lengkap. Misalnya, akun anak tidak dapat menerima pengaturan untuk beberapa kontrol dari satu kebijakan dan setelan untuk kontrol lain dari kebijakan lain. Saat Anda mengaitkan kebijakan dengan akun anak, pastikan kebijakan tersebut menentukan semua setelan yang Anda inginkan untuk digunakan oleh akun anak tersebut.
- Kebijakan konfigurasi tidak dapat dikembalikan — Tidak ada opsi untuk mengembalikan kebijakan konfigurasi setelah Anda mengaitkannya dengan akun atau OU. Misalnya, jika Anda mengaitkan kebijakan konfigurasi yang menonaktifkan CloudWatch kontrol dengan akun tertentu, lalu memisahkan kebijakan tersebut, CloudWatch kontrol akan terus dinonaktifkan di akun tersebut. Untuk mengaktifkan CloudWatch kontrol lagi, Anda dapat mengaitkan akun dengan kebijakan baru yang memungkinkan kontrol. Atau, Anda dapat mengubah akun menjadi dikelola sendiri dan mengaktifkan setiap CloudWatch kontrol di akun.

- Kebijakan konfigurasi berlaku di Wilayah asal Anda dan semua Wilayah tertaut — Kebijakan konfigurasi memengaruhi semua akun terkait di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang berlaku hanya di beberapa Wilayah ini dan bukan yang lain. Pengecualian untuk ini adalah kontrol yang menggunakan sumber daya global. Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal.

  Wilayah yang AWS diperkenalkan pada atau setelah 20 Maret 2019 dikenal sebagai Wilayah keikutsertaan. Anda harus mengaktifkan Wilayah tersebut untuk akun sebelum kebijakan konfigurasi berlaku di sana. Akun manajemen Organisasi dapat mengaktifkan Wilayah keikutsertaan untuk akun anggota. Untuk petunjuk tentang mengaktifkan Wilayah keikutsertaan, lihat Menentukan Wilayah AWS akun mana yang dapat digunakan dalam Panduan Referensi Manajemen AWS Akun.

  Jika kebijakan Anda mengonfigurasi kontrol yang tidak tersedia di Wilayah beranda atau satu atau beberapa Wilayah tertaut, CSPM Security Hub akan melewatkan konfigurasi kontrol di Wilayah yang tidak tersedia tetapi menerapkan konfigurasi di Wilayah tempat kontrol tersedia. Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.
- Kebijakan konfigurasi adalah sumber daya — Sebagai sumber daya, kebijakan konfigurasi memiliki Nama Sumber Daya Amazon (ARN) dan pengenal unik universal (UUID). ARN menggunakan format berikut:. `arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID` Konfigurasi yang dikelola sendiri tidak memiliki ARN atau UUID. Pengidentifikasi untuk konfigurasi yang dikelola sendiri adalah. `SELF_MANAGED_SECURITY_HUB`
- Standar multicloud tidak didukung dalam kebijakan konfigurasi — Kebijakan konfigurasi hanya dapat mencakup standar AWS keamanan dan kontrol. Standar multicloud, seperti CIS Azure Foundations Benchmark v4.0.0, dan kontrol terkaitnya (misalnya,`Azure.Storage.1`) tidak dapat dimasukkan dalam kebijakan konfigurasi. Jika Anda menyertakan ARN standar multicloud atau ID kontrol dalam kebijakan konfigurasi, permintaan akan mengembalikan file. `InvalidInputException` Untuk mengaktifkan atau mengkonfigurasi standar multicloud, gunakan mekanisme konfigurasi lokal langsung di yang diinginkan. Akun AWS

Jenis kebijakan konfigurasi

Setiap kebijakan konfigurasi menentukan setelan berikut:

- Mengaktifkan atau menonaktifkan Security Hub CSPM.

- Aktifkan satu atau lebih standar keamanan.
- Tunjukkan kontrol keamanan mana yang diaktifkan di seluruh standar yang diaktifkan. Anda dapat melakukannya dengan menyediakan daftar kontrol khusus yang harus diaktifkan, dan Security Hub CSPM menonaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis. Atau, Anda dapat memberikan daftar kontrol khusus yang harus dinonaktifkan, dan Security Hub CSPM mengaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis.
- Secara opsional, sesuaikan parameter untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Kebijakan konfigurasi pusat tidak menyertakan pengaturan AWS Config perekam. Anda harus mengaktifkan AWS Config dan mengaktifkan perekaman secara terpisah untuk sumber daya yang diperlukan agar Security Hub CSPM dapat menghasilkan temuan kontrol. Untuk informasi selengkapnya, lihat Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config.

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal.

Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.

Untuk daftar kontrol yang melibatkan sumber daya global, lihatKontrol yang menggunakan sumber daya global.

Kebijakan konfigurasi yang disarankan

Saat membuat kebijakan konfigurasi untuk pertama kalinya di konsol CSPM Security Hub, Anda memiliki opsi untuk memilih kebijakan yang direkomendasikan CSPM Security Hub.

Kebijakan yang direkomendasikan memungkinkan Security Hub CSPM, standar AWS Foundational Security Best Practices (FSBP), dan semua kontrol FSBP yang ada dan yang baru. Kontrol yang menerima parameter menggunakan nilai default. Kebijakan yang disarankan berlaku untuk root (semua akun dan OU, baik yang baru maupun yang sudah ada). Setelah membuat kebijakan yang disarankan untuk organisasi, Anda dapat memodifikasinya dari akun administrator

yang didelegasikan. Misalnya, Anda dapat mengaktifkan standar atau kontrol tambahan atau menonaktifkan kontrol FSBP tertentu. Untuk petunjuk tentang memodifikasi kebijakan konfigurasi, lihatMemperbarui kebijakan konfigurasi.

Kebijakan konfigurasi kustom

Alih-alih kebijakan yang disarankan, administrator yang didelegasikan dapat membuat hingga 20 kebijakan konfigurasi kustom. Anda dapat mengaitkan satu kebijakan kustom dengan seluruh organisasi atau kebijakan kustom yang berbeda dengan akun dan OU yang berbeda. Untuk kebijakan konfigurasi kustom, Anda menentukan pengaturan yang Anda inginkan. Misalnya, Anda dapat membuat kebijakan khusus yang memungkinkan FSBP, Tolok Ukur Yayasan Center for Internet Security (CIS AWS) v1.4.0, dan semua kontrol dalam standar tersebut kecuali kontrol Amazon Redshift. Tingkat perincian yang Anda gunakan dalam kebijakan konfigurasi khusus bergantung pada cakupan cakupan keamanan yang dimaksudkan di seluruh organisasi Anda.

> **Note**
>
> Anda tidak dapat mengaitkan kebijakan konfigurasi yang menonaktifkan CSPM Security Hub dengan akun administrator yang didelegasikan. Kebijakan semacam itu dapat dikaitkan dengan akun lain tetapi melewatkan asosiasi dengan administrator yang didelegasikan. Akun administrator yang didelegasikan mempertahankan konfigurasi saat ini.

Setelah membuat kebijakan konfigurasi kustom, Anda dapat beralih ke kebijakan konfigurasi yang disarankan dengan memperbarui kebijakan konfigurasi untuk mencerminkan konfigurasi yang disarankan. Namun, Anda tidak melihat pilihan untuk membuat kebijakan konfigurasi yang disarankan di konsol CSPM Security Hub setelah kebijakan pertama Anda dibuat.

Asosiasi kebijakan melalui aplikasi dan warisan

Saat Anda pertama kali ikut serta dalam konfigurasi pusat, organisasi Anda tidak memiliki asosiasi dan berperilaku dengan cara yang sama seperti sebelum ikut serta. Administrator yang didelegasikan kemudian dapat membuat asosiasi antara kebijakan konfigurasi atau perilaku dan akun yang dikelola sendiri, OU, atau root. Asosiasi dapat dibentuk melalui aplikasi atau warisan.

Dari akun administrator yang didelegasikan, Anda dapat langsung menerapkan kebijakan konfigurasi ke akun, OU, atau root. Atau, administrator yang didelegasikan dapat langsung menerapkan penunjukan yang dikelola sendiri ke akun, OU, atau root.

Dengan tidak adanya aplikasi langsung, akun atau OU mewarisi pengaturan induk terdekat yang memiliki kebijakan konfigurasi atau perilaku yang dikelola sendiri. Jika induk terdekat dikaitkan dengan kebijakan konfigurasi, anak mewarisi kebijakan tersebut dan hanya dapat dikonfigurasi oleh administrator yang didelegasikan dari Wilayah beranda. Jika orang tua terdekat dikelola sendiri, anak mewarisi perilaku yang dikelola sendiri dan memiliki kemampuan untuk menentukan pengaturannya sendiri di masing-masing. Wilayah AWS

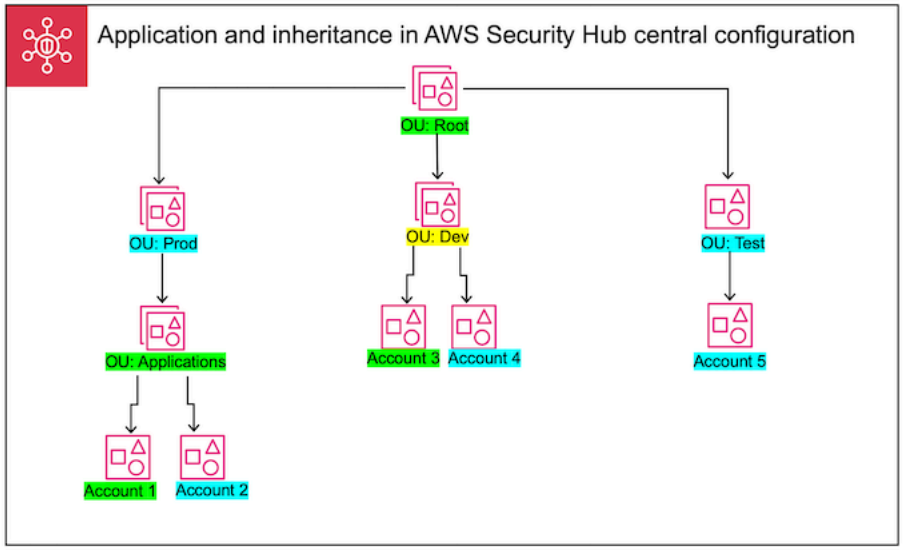
Aplikasi lebih diutamakan daripada warisan. Dengan kata lain, pewarisan tidak mengesampingkan kebijakan konfigurasi atau penunjukan yang dikelola sendiri yang telah diterapkan langsung oleh administrator yang didelegasikan ke akun atau OU.

Jika Anda langsung menerapkan kebijakan konfigurasi ke akun yang dikelola sendiri, kebijakan tersebut akan mengesampingkan penunjukan yang dikelola sendiri. Akun menjadi dikelola secara terpusat dan mengadopsi pengaturan yang tercermin dalam kebijakan konfigurasi.

Kami merekomendasikan langsung menerapkan kebijakan konfigurasi ke root. Jika Anda menerapkan kebijakan ke root, maka akun baru yang bergabung dengan organisasi Anda akan secara otomatis mewarisi kebijakan root kecuali Anda mengaitkannya dengan kebijakan yang berbeda atau menunjuknya sebagai dikelola sendiri.

Hanya satu kebijakan konfigurasi yang dapat dikaitkan dengan akun atau OU pada waktu tertentu, baik melalui aplikasi atau warisan. Ini dirancang untuk mencegah pengaturan yang bertentangan.

Diagram berikut menggambarkan bagaimana aplikasi kebijakan dan pewarisan bekerja dalam konfigurasi pusat.



Dalam contoh ini, node yang disorot dengan warna hijau memiliki kebijakan konfigurasi yang telah diterapkan padanya. Node yang disorot dengan warna biru tidak memiliki kebijakan konfigurasi yang telah diterapkan padanya. Sebuah simpul yang disorot dengan warna kuning telah ditetapkan sebagai dikelola sendiri. Setiap akun dan OU menggunakan konfigurasi berikut:

- OU:Root (Hijau) - OU ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- OU:Prod (Biru) - OU ini mewarisi kebijakan konfigurasi dari OU:Root.
- OU:Applications (Hijau) - OU ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 1 (Hijau) — Akun ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 2 (Biru) — Akun ini mewarisi kebijakan konfigurasi dari OU:Applications.
- OU:Dev (Kuning) - OU ini dikelola sendiri.
- Akun 3 (Hijau) — Akun ini menggunakan kebijakan konfigurasi yang telah diterapkan padanya.
- Akun 4 (Biru) — Akun ini mewarisi perilaku yang dikelola sendiri dari. OU:Dev
- OU:Test (Biru) — Akun ini mewarisi kebijakan konfigurasi dari OU:Root.
- Akun 5 (Biru) — Akun ini mewarisi kebijakan konfigurasi OU:Root karena induk langsungnya OU:Test, tidak terkait dengan kebijakan konfigurasi.

Menguji kebijakan konfigurasi

Untuk memastikan Anda memahami cara kerja kebijakan konfigurasi, sebaiknya buat satu kebijakan dan kaitkan dengan akun pengujian atau OU.

Untuk menguji kebijakan konfigurasi

1. Buat kebijakan konfigurasi khusus, dan verifikasi bahwa pengaturan yang ditentukan untuk pengaktifan, standar, dan kontrol CSPM Security Hub sudah benar. Untuk petunjuk, lihat Membuat dan mengaitkan kebijakan konfigurasi.
2. Terapkan kebijakan konfigurasi ke akun pengujian atau OU yang tidak memiliki akun anak atau OU.
3. Verifikasi bahwa akun pengujian atau OU menggunakan kebijakan konfigurasi dengan cara yang diharapkan di Wilayah asal Anda dan semua Wilayah yang ditautkan. Anda juga dapat memverifikasi bahwa semua akun dan OU lain di organisasi Anda tetap dikelola sendiri dan dapat mengubah pengaturan mereka sendiri di setiap Wilayah.

Setelah menguji kebijakan konfigurasi dalam satu akun atau OU, Anda dapat mengaitkannya dengan akun lain dan OU.

Membuat dan mengaitkan kebijakan konfigurasi

Akun administrator CSPM AWS Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi yang menentukan cara CSPM, standar, dan kontrol Security Hub dikonfigurasi dalam akun dan unit organisasi (OU) yang ditentukan. Kebijakan konfigurasi berlaku hanya setelah administrator yang didelegasikan mengaitkannya dengan setidaknya satu akun atau unit organisasi (OU), atau root. Administrator yang didelegasikan juga dapat mengaitkan konfigurasi yang dikelola sendiri dengan akun, OU, atau root.

Jika ini adalah pertama kalinya Anda membuat kebijakan konfigurasi, sebaiknya Cara kerja kebijakan konfigurasi di Security Hub CSPM tinjau terlebih dahulu.

> **Note**
>
> Kebijakan konfigurasi hanya mendukung AWS standar dan kontrol. Anda tidak dapat menyertakan standar multicloud (seperti CIS Azure Foundations Benchmark v4.0.0) atau kontrol Azure dalam kebijakan konfigurasi. Termasuk ARN standar multicloud atau pengembalian ID kontrol. `InvalidInputException` Untuk mengaktifkan atau mengkonfigurasi standar multicloud, gunakan mekanisme konfigurasi lokal langsung di yang diinginkan. Akun AWS

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk membuat dan mengaitkan kebijakan konfigurasi atau konfigurasi yang dikelola sendiri. Saat menggunakan konsol CSPM Security Hub, Anda dapat mengaitkan konfigurasi dengan beberapa akun atau OU secara bersamaan. Saat menggunakan Security Hub CSPM API atau AWS CLI, Anda dapat mengaitkan konfigurasi dengan hanya satu akun atau OU di setiap permintaan.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal.

Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.
Untuk daftar kontrol yang melibatkan sumber daya global, lihatKontrol yang menggunakan sumber daya global.

Security Hub CSPM console

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Di panel navigasi, pilih Konfigurasi dan tab Kebijakan. Kemudian, pilih Buat kebijakan.
3. Pada halaman Konfigurasi organisasi, jika ini adalah pertama kalinya Anda membuat kebijakan konfigurasi, Anda akan melihat tiga opsi di bawah Jenis konfigurasi. Jika Anda telah membuat setidaknya satu kebijakan konfigurasi, Anda hanya melihat opsi Kebijakan kustom.

   - Pilih Gunakan konfigurasi CSPM Security Hub yang AWS direkomendasikan di seluruh organisasi saya untuk menggunakan kebijakan yang kami rekomendasikan. Kebijakan yang direkomendasikan memungkinkan CSPM Security Hub di semua akun organisasi, mengaktifkan standar Praktik Terbaik Keamanan AWS Dasar (FSBP), dan memungkinkan semua kontrol FSBP baru dan yang sudah ada. Kontrol menggunakan nilai parameter default.
   - Pilih Saya belum siap untuk mengonfigurasi untuk membuat kebijakan konfigurasi nanti.
   - Pilih Kebijakan khusus untuk membuat kebijakan konfigurasi kustom. Tentukan apakah akan mengaktifkan atau menonaktifkan CSPM Security Hub, standar mana yang akan diaktifkan, dan kontrol mana yang akan diaktifkan di seluruh standar tersebut. Secara opsional, tentukan nilai parameter khusus untuk satu atau beberapa kontrol yang diaktifkan yang mendukung parameter kustom.
4. Di bagian Akun, pilih akun target, OU, atau root yang Anda inginkan untuk diterapkan oleh kebijakan konfigurasi Anda.

- Pilih Semua akun jika Anda ingin menerapkan kebijakan konfigurasi ke root. Ini termasuk semua akun dan OU di organisasi yang tidak memiliki kebijakan lain yang diterapkan atau diwariskan.
- Pilih Akun khusus jika Anda ingin menerapkan kebijakan konfigurasi ke akun atau OU tertentu. Masukkan ID akun, atau pilih akun dan OU dari struktur organisasi. Anda dapat menerapkan kebijakan ke maksimal 15 target (akun, OU, atau root) saat Anda membuatnya. Untuk menentukan angka yang lebih besar, edit kebijakan Anda setelah dibuat, dan terapkan ke target tambahan.
- Pilih Administrator yang didelegasikan hanya untuk menerapkan kebijakan konfigurasi ke akun administrator yang didelegasikan saat ini.

5. Pilih Berikutnya.
6. Pada halaman Tinjau dan terapkan, tinjau detail kebijakan konfigurasi Anda. Kemudian, pilih Buat kebijakan dan terapkan. Di Wilayah beranda dan Wilayah tertaut, tindakan ini mengesampingkan setelan konfigurasi akun yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi, atau warisan dari node induk. Akun turunan dan OU dari target yang diterapkan akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali secara khusus dikecualikan, dikelola sendiri, atau menggunakan kebijakan konfigurasi yang berbeda.

Security Hub CSPM API

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Memanggil CreateConfigurationPolicyAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.
2. Untuk`Name`, berikan nama unik untuk kebijakan konfigurasi. Secara opsional, untuk`Description`, berikan deskripsi untuk kebijakan konfigurasi.
3. Untuk `ServiceEnabled` bidang, tentukan apakah Anda ingin CSPM Security Hub diaktifkan atau dinonaktifkan dalam kebijakan konfigurasi ini.
4. Untuk `EnabledStandardIdentifiers` bidang, tentukan standar CSPM Security Hub mana yang ingin Anda aktifkan dalam kebijakan konfigurasi ini.
5. Untuk `SecurityControlsConfiguration` objek, tentukan kontrol mana yang ingin Anda aktifkan atau nonaktifkan dalam kebijakan konfigurasi ini. Memilih `EnabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan

diaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) dinonaktifkan. Memilih `DisabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan dinonaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) diaktifkan.

6. Secara opsional, untuk `SecurityControlCustomParameters` bidang, tentukan kontrol yang diaktifkan yang ingin Anda sesuaikan parameternya. Berikan `CUSTOM` `ValueType` bidang dan nilai parameter khusus untuk `Value` bidang tersebut. Nilai harus tipe data yang benar dan dalam rentang valid yang ditentukan oleh Security Hub CSPM. Hanya kontrol pilih yang mendukung nilai parameter khusus. Untuk informasi selengkapnya, lihat Memahami parameter kontrol di Security Hub CSPM.
7. Untuk menerapkan kebijakan konfigurasi Anda ke akun atau OU, panggil StartConfigurationPolicyAssociationAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
8. Untuk `ConfigurationPolicyIdentifier` bidang ini, berikan Nama Sumber Daya Amazon (ARN) atau pengenal unik universal (UUID) kebijakan. ARN dan UUID dikembalikan oleh API. `CreateConfigurationPolicy` Untuk konfigurasi yang dikelola sendiri, `ConfigurationPolicyIdentifier` bidangnya sama dengan`SELF_MANAGED_SECURITY_HUB`.
9. Untuk `Target` bidang, berikan OU, akun, atau ID root yang Anda inginkan untuk menerapkan kebijakan konfigurasi ini. Anda hanya dapat memberikan satu target di setiap permintaan API. Akun turunan dan OU dari target yang dipilih akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali mereka dikelola sendiri atau menggunakan kebijakan konfigurasi yang berbeda.

Contoh permintaan API untuk membuat kebijakan konfigurasi:

```
{
    "Name": "SampleConfigurationPolicy",
    "Description": "Configuration policy for production accounts",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
```

```
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

Contoh permintaan API untuk mengaitkan kebijakan konfigurasi:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

Untuk membuat dan mengaitkan kebijakan konfigurasi

1. Jalankan create-configuration-policyperintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.
2. Untuk`name`, berikan nama unik untuk kebijakan konfigurasi. Secara opsional, untuk`description`, berikan deskripsi untuk kebijakan konfigurasi.

3. Untuk `ServiceEnabled` bidang, tentukan apakah Anda ingin CSPM Security Hub diaktifkan atau dinonaktifkan dalam kebijakan konfigurasi ini.
4. Untuk `EnabledStandardIdentifiers` bidang, tentukan standar CSPM Security Hub mana yang ingin Anda aktifkan dalam kebijakan konfigurasi ini.
5. Untuk `SecurityControlsConfiguration` bidang, tentukan kontrol mana yang ingin Anda aktifkan atau nonaktifkan dalam kebijakan konfigurasi ini. Memilih `EnabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan diaktifkan. Kontrol lain yang merupakan bagian dari standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) dinonaktifkan. Memilih `DisabledSecurityControlIdentifiers` berarti bahwa kontrol yang ditentukan dinonaktifkan. Kontrol lain yang berlaku untuk standar Anda yang diaktifkan (termasuk kontrol yang baru dirilis) diaktifkan.
6. Secara opsional, untuk `SecurityControlCustomParameters` bidang, tentukan kontrol yang diaktifkan yang ingin Anda sesuaikan parameternya. Berikan `CUSTOM` `ValueType` bidang dan nilai parameter khusus untuk `Value` bidang tersebut. Nilai harus tipe data yang benar dan dalam rentang valid yang ditentukan oleh Security Hub CSPM. Hanya kontrol pilih yang mendukung nilai parameter khusus. Untuk informasi selengkapnya, lihat Memahami parameter kontrol di Security Hub CSPM.
7. Untuk menerapkan kebijakan konfigurasi Anda ke akun atau OU, jalankan start-configuration-policy-associationperintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
8. Untuk `configuration-policy-identifier` bidang, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi. ARN dan ID ini dikembalikan oleh perintah. `create-configuration-policy`
9. Untuk `target` bidang, berikan OU, akun, atau ID root yang Anda inginkan untuk menerapkan kebijakan konfigurasi ini. Anda hanya dapat memberikan satu target setiap kali Anda menjalankan perintah. Anak-anak dari target yang dipilih akan secara otomatis mewarisi kebijakan konfigurasi ini kecuali mereka dikelola sendiri atau menggunakan kebijakan konfigurasi yang berbeda.

Contoh perintah untuk membuat kebijakan konfigurasi:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
```

```
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}'
```

Contoh perintah untuk mengaitkan kebijakan konfigurasi:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}'
```

`StartConfigurationPolicyAssociation`API mengembalikan bidang yang disebut`AssociationStatus`. Bidang ini memberi tahu Anda apakah asosiasi kebijakan sedang tertunda atau dalam keadaan berhasil atau gagal. Diperlukan waktu hingga 24 jam agar status berubah dari `PENDING` ke `SUCCESS` atau`FAILURE`. Untuk informasi selengkapnya tentang status asosiasi, lihatMeninjau status asosiasi kebijakan konfigurasi.

Meninjau status dan detail kebijakan konfigurasi

Administrator CSPM AWS Security Hub yang didelegasikan dapat melihat kebijakan konfigurasi untuk organisasi dan detailnya. Ini termasuk akun dan unit organisasi (OU) mana yang terkait dengan kebijakan.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat kebijakan konfigurasi Anda.

Security Hub CSPM console

Untuk melihat kebijakan konfigurasi (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.

2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan untuk ikhtisar kebijakan konfigurasi Anda.
4. Pilih kebijakan konfigurasi, dan pilih Lihat detail untuk melihat detail tambahan tentangnya, termasuk akun dan OU yang terkait dengannya.

Security Hub CSPM API

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda, gunakan ListConfigurationPoliciespengoperasian API CSPM Security Hub. Jika Anda menggunakanAWS CLI, jalankan list-configuration-policiesperintah. Akun administrator CSPM Security Hub yang didelegasikan harus menjalankan operasi di Wilayah asal.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

Untuk melihat detail tentang kebijakan konfigurasi tertentu, gunakan GetConfigurationPolicyoperasi. Jika Anda menggunakanAWS CLI, jalankan get-configuration-policy. Akun administrator yang didelegasikan harus menjalankan operasi di Wilayah asal. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Untuk melihat daftar ringkasan semua kebijakan konfigurasi Anda dan asosiasi akunnya, gunakan ListConfigurationPolicyAssociationsoperasi tersebut. Jika Anda menggunakanAWS CLI, jalankan list-configuration-policy-associationsperintah. Akun administrator yang didelegasikan harus menjalankan operasi di Wilayah asal. Secara opsional, Anda dapat memberikan parameter pagination atau memfilter hasil berdasarkan ID kebijakan tertentu, jenis asosiasi, atau status asosiasi.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

Untuk melihat asosiasi untuk akun tertentu, gunakan GetConfigurationPolicyAssociationoperasi. Jika Anda menggunakanAWS CLI, jalankan get-configuration-policy-associationperintah. Akun

administrator yang didelegasikan harus menjalankan operasi di Wilayah asal. Untuk`target`, berikan nomor akun, ID OU, atau ID root.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

Meninjau status asosiasi kebijakan konfigurasi

Operasi API konfigurasi pusat berikut mengembalikan bidang yang disebut`AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Bidang ini dikembalikan baik ketika konfigurasi yang mendasarinya adalah kebijakan konfigurasi dan ketika itu adalah perilaku yang dikelola sendiri.

Nilai `AssociationStatus` memberi tahu Anda apakah asosiasi kebijakan tertunda atau dalam keadaan berhasil atau gagal untuk akun tertentu. Diperlukan waktu hingga 24 jam agar status berubah dari `PENDING` ke `SUCCESS` atau`FAILED`. Status `SUCCESS` berarti bahwa semua pengaturan yang ditentukan dalam kebijakan konfigurasi dikaitkan dengan akun. Status `FAILED` berarti bahwa satu atau beberapa setelan yang ditentukan dalam kebijakan konfigurasi gagal dikaitkan dengan akun. Meskipun `FAILED` berstatus, akun dapat dikonfigurasi sebagian sesuai dengan kebijakan. Misalnya, Anda dapat mencoba mengaitkan akun dengan kebijakan konfigurasi yang mengaktifkan CSPM Security Hub, mengaktifkan Praktik Terbaik Keamanan AWS Dasar, dan menonaktifkan. CloudTrail.1 Dua pengaturan awal bisa berhasil, tetapi CloudTrail.1 pengaturannya bisa gagal. Dalam contoh ini, status asosiasi `FAILED` meskipun beberapa pengaturan telah dikonfigurasi dengan benar.

Status asosiasi OU orang tua atau root tergantung pada status anak-anaknya. Jika status asosiasi semua anak adalah`SUCCESS`, status asosiasi orang tua adalah`SUCCESS`. Jika status asosiasi satu atau lebih anak adalah`FAILED`, status asosiasi orang tua adalah`FAILED`.

Nilai `AssociationStatus` tergantung pada status asosiasi kebijakan di semua Wilayah terkait. Jika asosiasi berhasil di Wilayah asal dan semua Daerah terkait, nilainya `AssociationStatus` adalah`SUCCESS`. Jika asosiasi gagal di satu atau lebih Wilayah ini, nilainya `AssociationStatus` adalah`FAILED`.

Perilaku berikut juga berdampak pada nilai`AssociationStatus`:

- Jika targetnya adalah OU orang tua atau root, ia memiliki `AssociationStatus` dari `SUCCESS` atau `FAILED` hanya ketika semua anak memiliki `FAILED` status `SUCCESS` atau. Jika status asosiasi akun turunan atau OU berubah (misalnya, saat Wilayah tertaut ditambahkan atau dihapus) setelah Anda pertama kali mengaitkan induk dengan konfigurasi, perubahan tersebut tidak akan memperbarui status asosiasi induk kecuali Anda menjalankan `StartConfigurationPolicyAssociation` API lagi.
- Jika targetnya adalah akun, ia memiliki `AssociationStatus` dari `SUCCESS` atau `FAILED` hanya jika asosiasi memiliki hasil dari `SUCCESS` atau `FAILED` di Wilayah asal dan semua Wilayah yang ditautkan. Jika status asosiasi akun target berubah (misalnya, saat Wilayah tertaut ditambahkan atau dihapus) setelah Anda pertama kali mengaitkannya dengan konfigurasi, status asosiasinya akan diperbarui. Namun, perubahan tidak memperbarui status asosiasi induk kecuali Anda memanggil `StartConfigurationPolicyAssociation` API lagi.

Jika Anda menambahkan Wilayah tertaut baru, Security Hub CSPM mereplikasi asosiasi Anda yang ada di`PENDING`,`SUCCESS`, atau `FAILED` negara bagian di Wilayah baru.

Bahkan ketika status asosiasi adalah`SUCCESS`, status pemberdayaan standar yang merupakan bagian dari kebijakan dapat beralih ke keadaan yang tidak lengkap. Dalam hal ini, Security Hub CSPM tidak dapat menghasilkan temuan untuk kontrol standar. Untuk informasi selengkapnya, lihat Memeriksa status standar.

Memecahkan masalah kegagalan asosiasi

Di AWS Security Hub CSPM, asosiasi kebijakan konfigurasi mungkin gagal karena alasan umum berikut.

- Akun manajemen Organisasi bukan anggota — Jika Anda ingin mengaitkan kebijakan konfigurasi dengan akun manajemen Organizations, akun tersebut harus sudah mengaktifkan AWS Security Hub CSPM. Ini membuat akun manajemen menjadi akun anggota dalam organisasi.
- AWS Configtidak diaktifkan atau dikonfigurasi dengan benar — Untuk mengaktifkan standar dalam kebijakan konfigurasi, AWS Config harus diaktifkan dan dikonfigurasi untuk merekam sumber daya yang relevan.
- Harus dikaitkan dari akun administrator yang didelegasikan — Anda hanya dapat mengaitkan kebijakan dengan akun target dan OU saat Anda masuk ke akun administrator CSPM Security Hub yang didelegasikan.

- Harus dikaitkan dari wilayah asal — Anda hanya dapat mengaitkan kebijakan dengan akun target dan OU saat Anda masuk ke Wilayah asal Anda.
- Opt-in Wilayah tidak diaktifkan — Asosiasi kebijakan gagal untuk akun anggota atau OU di Wilayah tertaut jika itu adalah Wilayah keikutsertaan yang belum diaktifkan oleh administrator yang didelegasikan. Anda dapat mencoba lagi setelah mengaktifkan Region dari akun administrator yang didelegasikan.
- Akun anggota ditangguhkan — Asosiasi kebijakan gagal jika Anda mencoba mengaitkan kebijakan dengan akun anggota yang ditangguhkan.

Memperbarui kebijakan konfigurasi

Setelah membuat kebijakan konfigurasi, akun administrator CSPM AWS Security Hub yang didelegasikan dapat memperbarui detail kebijakan dan asosiasi kebijakan. Saat detail kebijakan diperbarui, akun yang terkait dengan kebijakan konfigurasi secara otomatis mulai menggunakan kebijakan yang diperbarui.

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihatMemahami konfigurasi pusat di Security Hub CSPM.

> **Note**
>
> Kebijakan konfigurasi hanya mendukung AWS standar dan kontrol. Anda tidak dapat menyertakan standar multicloud (seperti CIS Azure Foundations Benchmark v4.0.0) atau kontrol Azure dalam kebijakan konfigurasi. Termasuk ARN standar multicloud atau pengembalian ID kontrol. `InvalidInputException` Untuk mengaktifkan atau mengkonfigurasi standar multicloud, gunakan mekanisme konfigurasi lokal langsung di yang diinginkan. Akun AWS

Administrator yang didelegasikan dapat memperbarui setelan kebijakan berikut:

- Mengaktifkan atau menonaktifkan Security Hub CSPM.
- Aktifkan satu atau lebih standar keamanan.
- Tunjukkan kontrol keamanan mana yang diaktifkan di seluruh standar yang diaktifkan. Anda dapat melakukannya dengan menyediakan daftar kontrol khusus yang harus diaktifkan, dan Security Hub CSPM menonaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis. Atau, Anda

dapat memberikan daftar kontrol khusus yang harus dinonaktifkan, dan Security Hub CSPM mengaktifkan semua kontrol lainnya, termasuk kontrol baru saat dirilis.

- Secara opsional, sesuaikan parameter untuk memilih kontrol yang diaktifkan di seluruh standar yang diaktifkan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memperbarui kebijakan konfigurasi.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal.
> Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.
> Untuk daftar kontrol yang melibatkan sumber daya global, lihatKontrol yang menggunakan sumber daya global.

Console

Untuk memperbarui kebijakan konfigurasi

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Pilih kebijakan konfigurasi yang ingin Anda edit, lalu pilih Edit. Jika diinginkan, edit pengaturan kebijakan. Biarkan bagian ini seolah-olah Anda ingin menjaga pengaturan kebijakan tidak berubah.

5. Pilih Berikutnya. Jika diinginkan, edit asosiasi kebijakan. Biarkan bagian ini seolah-olah Anda ingin menjaga agar asosiasi kebijakan tidak berubah. Anda dapat mengaitkan atau memisahkan kebijakan dengan maksimal 15 target (akun, OU, atau root) saat Anda memperbaruinya.
6. Pilih Berikutnya.
7. Tinjau perubahan Anda, lalu pilih Simpan dan terapkan. Di Wilayah beranda dan Wilayah tertaut, tindakan ini mengesampingkan setelan konfigurasi akun yang ada yang terkait dengan kebijakan konfigurasi ini. Akun dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi, atau warisan dari node induk.

API

Untuk memperbarui kebijakan konfigurasi

1. Untuk memperbarui setelan dalam kebijakan konfigurasi, panggil UpdateConfigurationPolicyAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
2. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Berikan nilai yang diperbarui untuk bidang di bawah`ConfigurationPolicy`. Secara opsional, Anda juga dapat memberikan alasan untuk pembaruan.
4. Untuk menambahkan asosiasi baru untuk kebijakan konfigurasi ini, panggil StartConfigurationPolicyAssociationAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda. Untuk menghapus satu atau beberapa asosiasi saat ini, panggil StartConfigurationPolicyDisassociationAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
5. Untuk `ConfigurationPolicyIdentifier` bidang, berikan ARN atau ID kebijakan konfigurasi yang asosiasinya ingin Anda perbarui.
6. Untuk `Target` bidang, berikan akun, OU, atau ID root yang ingin Anda kaitkan atau lepaskan. Tindakan ini mengesampingkan asosiasi kebijakan sebelumnya untuk OU atau akun tertentu.

> **Note**
>
> Saat Anda menjalankan `UpdateConfigurationPolicy` API, Security Hub CSPM melakukan penggantian daftar lengkap untuk`EnabledStandardIdentifiers`,, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, dan bidang. `SecurityControlCustomParameters` Setiap kali Anda menjalankan API ini, berikan daftar lengkap standar yang ingin Anda aktifkan dan daftar lengkap kontrol yang ingin Anda aktifkan atau nonaktifkan dan sesuaikan parameternya.

Contoh permintaan API untuk memperbarui kebijakan konfigurasi:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Description": "Updated configuration policy",
    "UpdatedReason": "Disabling CloudWatch.1",
    "ConfigurationPolicy": {
        "SecurityHub": {
             "ServiceEnabled": true,
             "EnabledStandardIdentifiers": [
                    "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
                    "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
                ],
            "SecurityControlsConfiguration": {
                "DisabledSecurityControlIdentifiers": [
                    "CloudTrail.2",
                    "CloudWatch.1"
                ],
                "SecurityControlCustomParameters": [
                    {
                        "SecurityControlId": "ACM.1",
                        "Parameters": {
                            "daysToExpiration": {
                                "ValueType": "CUSTOM",
                                "Value": {
                                    "Integer": 15
                                }
                            }
                        }
```

```
                    }
                ]
            }
        }
    }
}
```

AWS CLI

Untuk memperbarui kebijakan konfigurasi

1. Untuk memperbarui pengaturan dalam kebijakan konfigurasi, jalankan update-configuration-policyperintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda.
2. Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Berikan nilai yang diperbarui untuk bidang di bawah`configuration-policy`. Secara opsional, Anda juga dapat memberikan alasan untuk pembaruan.
4. Untuk menambahkan asosiasi baru untuk kebijakan konfigurasi ini, jalankan start-configuration-policy-associationperintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah beranda. Untuk menghapus satu atau beberapa asosiasi saat ini, jalankan start-configuration-policy-disassociationperintah dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah rumah.
5. Untuk `configuration-policy-identifier` bidang, berikan ARN atau ID kebijakan konfigurasi yang asosiasinya ingin Anda perbarui.
6. Untuk `target` bidang, berikan akun, OU, atau ID root yang ingin Anda kaitkan atau lepaskan. Tindakan ini mengesampingkan asosiasi kebijakan sebelumnya untuk OU atau akun tertentu.

> **Note**
>
> Saat Anda menjalankan `update-configuration-policy` perintah, Security Hub CSPM melakukan penggantian daftar lengkap untuk`EnabledStandardIdentifiers`,, `EnabledSecurityControlIdentifiersDisabledSecurityControlIdentifiers`, dan `SecurityControlCustomParameters` bidang. Setiap kali Anda menjalankan

perintah ini, berikan daftar lengkap standar yang ingin Anda aktifkan dan daftar lengkap kontrol yang ingin Anda aktifkan atau nonaktifkan dan sesuaikan parameternya.

Contoh perintah untuk memperbarui kebijakan konfigurasi:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}}}'
```

`StartConfigurationPolicyAssociation`API mengembalikan bidang yang disebut`AssociationStatus`. Bidang ini memberi tahu Anda apakah asosiasi kebijakan sedang tertunda atau dalam keadaan berhasil atau gagal. Diperlukan waktu hingga 24 jam agar status berubah dari `PENDING` ke `SUCCESS` atau`FAILURE`. Untuk informasi selengkapnya tentang status asosiasi, lihatMeninjau status asosiasi kebijakan konfigurasi.

Menghapus kebijakan konfigurasi

Setelah membuat kebijakan konfigurasi, administrator CSPM AWS Security Hub yang didelegasikan dapat menghapusnya. Atau, administrator yang didelegasikan dapat mempertahankan kebijakan, tetapi memisahkannya dari akun tertentu atau unit organisasi (OU), atau dari root. Untuk petunjuk tentang pemutusan kebijakan, lihat. Memutuskan konfigurasi dari targetnya

Untuk informasi latar belakang tentang manfaat konfigurasi pusat dan cara kerjanya, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Bagian ini menjelaskan cara menghapus kebijakan konfigurasi.

Saat Anda menghapus kebijakan konfigurasi, kebijakan tersebut tidak ada lagi untuk organisasi Anda. Akun target, OU, dan root organisasi tidak dapat lagi menggunakan kebijakan konfigurasi. Target yang dikaitkan dengan kebijakan konfigurasi yang dihapus mewarisi kebijakan konfigurasi induk terdekat, atau dikelola sendiri jika induk terdekat dikelola sendiri. Jika Anda ingin target menggunakan konfigurasi yang berbeda, Anda dapat mengaitkan target dengan kebijakan konfigurasi baru. Untuk informasi selengkapnya, lihat Membuat dan mengaitkan kebijakan konfigurasi.

Sebaiknya buat dan kaitkan setidaknya satu kebijakan konfigurasi dengan organisasi Anda untuk memberikan cakupan keamanan yang memadai.

Sebelum Anda dapat menghapus kebijakan konfigurasi, Anda harus memisahkan kebijakan dari akun, OU, atau root yang saat ini berlaku.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus kebijakan konfigurasi.

Console

Untuk menghapus kebijakan konfigurasi

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pilih tab Kebijakan. Pilih kebijakan konfigurasi yang ingin Anda hapus, lalu pilih Hapus. Jika kebijakan konfigurasi masih terkait dengan akun atau OU apa pun, Anda diminta untuk terlebih dahulu memisahkan kebijakan dari target tersebut sebelum dapat menghapusnya.
4. Tinjau pesan konfirmasi. Masukkan**`confirm`**, dan pilih Hapus.

API

Untuk menghapus kebijakan konfigurasi

Memanggil DeleteConfigurationPolicyAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.

Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda hapus. Jika Anda menerima `ConflictException` kesalahan, kebijakan konfigurasi masih

berlaku untuk akun atau OU di organisasi Anda. Untuk mengatasi kesalahan, putuskan kebijakan konfigurasi dari akun ini atau OU sebelum mencoba menghapusnya.

Contoh permintaan API untuk menghapus kebijakan konfigurasi:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Untuk menghapus kebijakan konfigurasi

Jalankan delete-configuration-policyperintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.

Berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda hapus. Jika Anda menerima `ConflictException` kesalahan, kebijakan konfigurasi masih berlaku untuk akun atau OU di organisasi Anda. Untuk mengatasi kesalahan, putuskan kebijakan konfigurasi dari akun ini atau OU sebelum mencoba menghapusnya.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Memutuskan konfigurasi dari targetnya

Dari akun administrator CSPM AWS Security Hub yang didelegasikan, Anda dapat memisahkan kebijakan konfigurasi atau konfigurasi yang dikelola sendiri dari akun, OU, atau root. Disassociation mempertahankan kebijakan untuk penggunaan di masa mendatang, tetapi menghapus asosiasi yang ada dari akun tertentu, OU, atau root. Anda hanya dapat memisahkan konfigurasi yang diterapkan secara langsung, bukan konfigurasi yang diwariskan. Untuk mengubah konfigurasi yang diwariskan, Anda dapat menerapkan kebijakan konfigurasi atau perilaku yang dikelola sendiri ke akun atau OU yang terpengaruh. Anda juga dapat menerapkan kebijakan konfigurasi baru, yang mencakup modifikasi yang Anda inginkan, ke induk terdekat.

Disassociation tidak menghapus kebijakan konfigurasi. Kebijakan ini disimpan di akun Anda, sehingga Anda dapat mengaitkannya dengan target lain di organisasi Anda. Untuk petunjuk tentang menghapus kebijakan konfigurasi, lihatMenghapus kebijakan konfigurasi. Ketika disasosiasi selesai, target yang terpengaruh mewarisi kebijakan konfigurasi atau perilaku yang dikelola sendiri dari induk terdekat. Jika tidak ada konfigurasi yang dapat diwariskan, target mempertahankan pengaturan yang dimilikinya sebelum disasosiasi tetapi menjadi dikelola sendiri.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun, OU, atau root dari konfigurasi saat ini.

Console

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensional akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Di panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Pada tab Organizations, pilih akun, OU, atau root yang ingin Anda lepaskan dari konfigurasi saat ini. Pilih Edit.
4. Pada halaman Tentukan konfigurasi, untuk Manajemen, pilih Kebijakan diterapkan jika Anda ingin administrator yang didelegasikan dapat menerapkan kebijakan secara langsung ke target. Pilih Inherited jika Anda ingin target mewarisi konfigurasi induk terdekatnya. Dalam salah satu kasus ini, administrator yang didelegasikan mengontrol pengaturan untuk target. Pilih Self-managedapakah Anda ingin akun atau OU mengontrol pengaturannya sendiri.
5. Setelah meninjau perubahan Anda, pilih Berikutnya dan Terapkan. Tindakan ini mengesampingkan konfigurasi akun atau OU yang ada dalam cakupan, jika konfigurasi tersebut bertentangan dengan pilihan Anda saat ini.

API

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Memanggil StartConfigurationPolicyDisassociationAPI dari akun administrator yang didelegasikan CSPM Security Hub di Wilayah asal.

2. Untuk`ConfigurationPolicyIdentifier`, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda putuskan. Sediakan bidang ini `SELF_MANAGED_SECURITY_HUB` untuk memisahkan perilaku yang dikelola sendiri.
3. Untuk`Target`, berikan akun, OU, atau root yang ingin Anda memisahkan dari kebijakan konfigurasi ini.

Contoh permintaan API untuk memisahkan kebijakan konfigurasi:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Untuk memisahkan akun atau OU dari konfigurasi saat ini

1. Jalankan start-configuration-policy-disassociationperintah dari akun administrator yang didelegasikan CSPM Security Hub di wilayah rumah.
2. Untuk`configuration-policy-identifier`, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda putuskan. Sediakan bidang ini `SELF_MANAGED_SECURITY_HUB` untuk memisahkan perilaku yang dikelola sendiri.
3. Untuk`target`, berikan akun, OU, atau root yang ingin Anda memisahkan dari kebijakan konfigurasi ini.

Contoh perintah untuk memisahkan kebijakan konfigurasi:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Mengkonfigurasi standar atau kontrol dalam konteks

Bila Anda menggunakan konfigurasi pusat di AWS Security Hub CSPM, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi yang menentukan cara CSPM Security Hub, standar keamanan, dan kontrol keamanan dikonfigurasi untuk organisasi. Administrator yang didelegasikan dapat mengaitkan kebijakan dengan akun tertentu dan unit organisasi (OU). Kebijakan berlaku di Wilayah asal Anda dan semua Wilayah terkait. Administrator yang didelegasikan dapat memperbarui kebijakan konfigurasi seperlunya.

Di konsol CSPM Security Hub, administrator yang didelegasikan dapat memperbarui kebijakan konfigurasi dengan dua cara—dari halaman Konfigurasi, atau dalam konteks alur kerja yang ada. Yang terakhir ini dapat bermanfaat karena, saat Anda melihat temuan keamanan, Anda dapat menemukan standar dan kontrol mana yang paling relevan dengan lingkungan Anda dan mengonfigurasinya pada saat yang bersamaan.

In-context konfigurasi hanya tersedia di konsol CSPM Security Hub. Secara terprogram, administrator yang didelegasikan harus memanggil UpdateConfigurationPolicypengoperasian Security Hub CSPM API untuk mengubah cara standar atau kontrol tertentu dikonfigurasi dalam organisasi.

Ikuti langkah-langkah ini untuk mengonfigurasi standar atau kontrol CSPM Security Hub dalam konteks.

Untuk mengkonfigurasi standar atau kontrol dalam konteks (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Di panel navigasi, pilih salah satu opsi berikut:

   - Untuk mengkonfigurasi standar, pilih Standar keamanan, dan pilih standar tertentu.
   - Untuk mengonfigurasi kontrol, pilih Kontrol, dan pilih kontrol tertentu.
3. Konsol mencantumkan kebijakan konfigurasi CSPM Security Hub yang ada dan status standar atau kontrol yang dipilih di masing-masing. Pilih opsi untuk mengaktifkan atau menonaktifkan standar atau kontrol di setiap kebijakan konfigurasi yang ada. Untuk kontrol, Anda juga dapat memilih untuk menyesuaikan parameter kontrol. Anda tidak dapat membuat kebijakan baru selama konfigurasi dalam konteks. Untuk membuat kebijakan baru, Anda harus pergi ke halaman Konfigurasi, pilih tab Kebijakan, lalu pilih Buat kebijakan.
4. Setelah melakukan perubahan, pilih Berikutnya.

5. Tinjau perubahan Anda, dan pilih Terapkan. Pembaruan memengaruhi semua akun dan OU yang terkait dengan kebijakan konfigurasi yang diubah. Pembaruan juga berlaku di Wilayah asal dan semua Wilayah terkait.

Menonaktifkan konfigurasi pusat di Security Hub CSPM

Saat Anda menonaktifkan konfigurasi pusat di AWS Security Hub CSPM, administrator yang didelegasikan kehilangan kemampuan untuk mengonfigurasi CSPM Security Hub, standar keamanan, dan kontrol keamanan di beberapa unit organisasi (OU)Akun AWS, dan. Wilayah AWS Sebagai gantinya, Anda harus mengonfigurasi sebagian besar pengaturan secara terpisah untuk setiap akun di setiap Wilayah.

> **Important**
>
> Sebelum Anda dapat menonaktifkan konfigurasi pusat, Anda harus terlebih dahulu memisahkan akun dan OU Anda dari konfigurasi mereka saat ini, apakah itu kebijakan konfigurasi atau perilaku yang dikelola sendiri.
> Sebelum Anda dapat menonaktifkan konfigurasi pusat, Anda juga harus menghapus kebijakan konfigurasi yang ada.

Ketika Anda menonaktifkan konfigurasi pusat, perubahan berikut terjadi:

- Administrator yang didelegasikan tidak dapat lagi membuat kebijakan konfigurasi untuk organisasi.
- Akun yang memiliki kebijakan konfigurasi yang diterapkan atau diwariskan mempertahankan pengaturan mereka saat ini, tetapi menjadi dikelola sendiri.
- Organisasi Anda beralih ke konfigurasi lokal. Di bawah konfigurasi lokal, sebagian besar pengaturan CSPM Security Hub harus dikonfigurasi secara terpisah di setiap akun organisasi dan Wilayah. Administrator yang didelegasikan dapat memilih untuk mengaktifkan CSPM Security Hub secara otomatis, standar keamanan default, dan semua kontrol yang merupakan bagian dari standar default di akun organisasi baru. Standar default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Pengaturan ini hanya berlaku di Wilayah saat ini dan hanya memengaruhi akun organisasi baru. Administrator yang didelegasikan tidak dapat mengubah standar mana yang default. Konfigurasi lokal tidak mendukung penggunaan kebijakan konfigurasi atau konfigurasi di tingkat OU.

Identitas akun administrator yang didelegasikan tetap sama ketika Anda berhenti menggunakan konfigurasi pusat. Wilayah asal Anda dan Wilayah terkait juga tetap sama (Wilayah asal Anda sekarang disebut Wilayah agregasi, dan dapat digunakan untuk menemukan agregasi).

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk berhenti menggunakan konfigurasi pusat dan beralih ke konfigurasi lokal.

Security Hub CSPM console

Untuk menonaktifkan konfigurasi pusat (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensil akun administrator CSPM Security Hub yang didelegasikan di Wilayah asal.
2. Pada panel navigasi, pilih Pengaturan dan Konfigurasi.
3. Di bagian Ikhtisar, pilih Edit.
4. Di kotak Edit konfigurasi organisasi, pilih Konfigurasi lokal. Jika belum melakukannya, Anda diminta untuk memisahkan dan menghapus kebijakan konfigurasi Anda saat ini sebelum Anda dapat menghentikan konfigurasi pusat. Akun atau OU yang ditetapkan sebagai dikelola sendiri harus dipisahkan dari konfigurasi yang dikelola sendiri. Anda dapat melakukan ini di konsol dengan mengubah jenis manajemen setiap akun yang dikelola sendiri atau OU menjadi dikelola secara terpusat dan Mewarisi dari organisasi saya.
5. Secara opsional, pilih pengaturan default konfigurasi lokal untuk akun organisasi baru.
6. Pilih Konfirmasi.

Security Hub CSPM API

Untuk menonaktifkan konfigurasi pusat (API)

1. Memanggil UpdateOrganizationConfigurationAPI.
2. Atur `ConfigurationType` bidang di `OrganizationConfiguration` objek ke`LOCAL`. API menampilkan kesalahan jika Anda memiliki kebijakan konfigurasi atau asosiasi kebijakan yang ada. Untuk memisahkan kebijakan konfigurasi, panggil API. `StartConfigurationPolicyDisassociation` Untuk menghapus kebijakan konfigurasi, panggil `DeleteConfigurationPolicy` API.

3. Jika Anda ingin mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru, setel `AutoEnable` kolom ke. `true` Secara default, nilai bidang ini adalah`false`, dan CSPM Security Hub tidak diaktifkan secara otomatis di akun organisasi baru. Secara opsional, jika Anda ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `AutoEnableStandards` bidang ke`DEFAULT`. Ini nilai default. Jika Anda tidak ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `AutoEnableStandards` bidang tersebut`NONE`.

Contoh permintaan API:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

Untuk menonaktifkan konfigurasi pusat (AWS CLI)

1. Jalankan perintah update-organization-configuration.
2. Atur `ConfigurationType` bidang di `organization-configuration` objek ke`LOCAL`. Perintah mengembalikan kesalahan jika Anda memiliki kebijakan konfigurasi atau asosiasi kebijakan yang ada. Untuk memisahkan kebijakan konfigurasi, jalankan `start-configuration-policy-disassociation` perintah. Untuk menghapus kebijakan konfigurasi, jalankan `delete-configuration-policy` perintah.
3. Jika Anda ingin mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru, sertakan parameternya`auto-enable`. Secara default, nilai parameter ini adalah`no-auto-enable`, dan CSPM Security Hub tidak diaktifkan secara otomatis di akun organisasi baru. Secara opsional, jika Anda ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `auto-enable-standards` bidang ke`DEFAULT`. Ini nilai default. Jika Anda tidak ingin mengaktifkan standar keamanan default secara otomatis di akun organisasi baru, setel `auto-enable-standards` bidang tersebut`NONE`.

```
aws securityhub --region us-east-1 update-organization-configuration \
```

```
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Mengelola akun administrator dan anggota di Security Hub CSPM

Jika AWS lingkungan Anda memiliki beberapa akun, Anda dapat memperlakukan akun yang menggunakan AWS Security Hub CSPM sebagai akun anggota dan mengaitkannya dengan satu akun administrator. Administrator dapat memantau postur keamanan Anda secara keseluruhan dan mengambil tindakan yang diizinkan pada akun anggota. Administrator juga dapat melakukan berbagai tugas manajemen akun dan administrasi dalam skala besar, seperti memantau perkiraan biaya penggunaan dan menilai kuota akun.

Anda dapat mengaitkan akun anggota dengan administrator dalam dua cara, dengan mengintegrasikan Security Hub CSPM dengan AWS Organizations atau dengan mengirim dan menerima undangan keanggotaan secara manual di Security Hub CSPM.

Mengelola akun denganAWS Organizations

AWS Organizationsadalah layanan manajemen akun global yang memungkinkan AWS administrator untuk mengkonsolidasikan dan mengelola beberapa. Akun AWS Ini menyediakan manajemen akun dan fitur penagihan terkonsolidasi yang dirancang untuk mendukung kebutuhan anggaran, keamanan, dan kepatuhan. Ini ditawarkan tanpa biaya tambahan, dan terintegrasi dengan beberapa, termasuk AWS Security Hub CSPMLayanan AWS, Amazon Macie, dan Amazon. GuardDuty Untuk informasi selengkapnya, silakan lihat Panduan Pengguna AWS Organizations.

Saat Anda mengintegrasikan CSPM Security Hub danAWS Organizations, akun manajemen Organizations menunjuk administrator yang didelegasikan CSPM Security Hub. Security Hub CSPM secara otomatis diaktifkan di akun administrator yang didelegasikan Wilayah AWS di mana ia ditunjuk.

Setelah menunjuk administrator yang didelegasikan, kami sarankan mengelola akun di Security Hub CSPM dengan konfigurasi pusat. Ini adalah cara paling efisien untuk menyesuaikan Security Hub CSPM dan memastikan cakupan keamanan yang memadai untuk organisasi Anda.

Konfigurasi pusat memungkinkan administrator yang didelegasikan menyesuaikan CSPM Security Hub di beberapa akun organisasi dan Wilayah daripada mengonfigurasi. Region-by-Region Anda dapat membuat kebijakan konfigurasi untuk seluruh organisasi, atau membuat kebijakan konfigurasi

yang berbeda untuk akun dan OU yang berbeda. Kebijakan menentukan apakah CSPM Security Hub diaktifkan atau dinonaktifkan di akun terkait dan standar dan kontrol keamanan mana yang diaktifkan.

Administrator yang didelegasikan dapat menetapkan akun sebagai dikelola secara terpusat atau dikelola sendiri. Akun yang dikelola secara terpusat hanya dapat dikonfigurasi oleh administrator yang didelegasikan. Self-managed akun dapat menentukan pengaturan mereka sendiri.

Jika Anda tidak ikut serta dalam konfigurasi pusat, administrator yang didelegasikan memiliki kemampuan yang lebih terbatas untuk mengonfigurasi CSPM Security Hub, yang disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan dapat secara otomatis mengaktifkan CSPM Security Hub dan standar keamanan default di akun organisasi baru di Wilayah saat ini. Namun, akun yang ada tidak menggunakan pengaturan ini, sehingga penyimpangan konfigurasi dapat terjadi setelah akun bergabung dengan organisasi.

Selain pengaturan akun baru ini, konfigurasi lokal bersifat spesifik akun dan. Region-specific Setiap akun organisasi harus mengonfigurasi layanan, standar, dan kontrol CSPM Security Hub secara terpisah di setiap Wilayah. Konfigurasi lokal juga tidak mendukung penggunaan kebijakan konfigurasi.

Mengelola akun secara manual dengan undangan

Anda harus mengelola akun anggota secara manual berdasarkan undangan di Security Hub CSPM jika Anda memiliki akun mandiri atau jika Anda tidak berintegrasi dengan Organizations. Akun mandiri tidak dapat diintegrasikan dengan Organizations, jadi Anda perlu mengelolanya secara manual. Kami merekomendasikan untuk mengintegrasikan dengan AWS Organizations dan menggunakan konfigurasi pusat jika Anda menambahkan akun tambahan di masa mendatang.

Saat Anda menggunakan manajemen akun manual, Anda menetapkan akun untuk menjadi administrator CSPM Security Hub. Akun administrator dapat melihat data di akun anggota dan mengambil tindakan tertentu pada temuan akun anggota. Administrator CSPM Security Hub mengundang akun lain untuk menjadi akun anggota, dan hubungan administrator-anggota terbentuk ketika akun calon anggota menerima undangan.

Manajemen akun manual tidak mendukung penggunaan kebijakan konfigurasi. Tanpa kebijakan konfigurasi, administrator tidak dapat menyesuaikan CSPM Security Hub secara terpusat dengan mengonfigurasi pengaturan variabel untuk akun yang berbeda. Sebagai gantinya, setiap akun organisasi harus mengaktifkan dan mengkonfigurasi CSPM Security Hub untuk dirinya sendiri secara terpisah di setiap Wilayah. Ini dapat membuatnya lebih sulit dan memakan waktu untuk memastikan cakupan keamanan yang memadai di semua akun dan Wilayah tempat Anda menggunakan Security

Hub CSPM. Ini juga dapat menyebabkan penyimpangan konfigurasi karena akun anggota dapat menentukan pengaturan mereka sendiri tanpa masukan dari administrator.

Untuk mengelola akun berdasarkan undangan, lihatMengelola akun dengan undangan di Security Hub CSPM.

Rekomendasi untuk mengelola beberapa akun di Security Hub CSPM

Bagian berikut merangkum beberapa batasan dan rekomendasi yang perlu diingat saat mengelola akun anggota di AWS Security Hub CSPM.

Jumlah maksimum akun anggota

Jika Anda menggunakan integrasi denganAWS Organizations, Security Hub CSPM mendukung hingga 10.000 akun anggota per akun administrator yang didelegasikan di masing-masing akun. Wilayah AWS Jika Anda mengaktifkan dan mengelola Security Hub CSPM secara manual, Security Hub CSPM mendukung hingga 1.000 undangan akun anggota per akun administrator di setiap Wilayah.

Membuat hubungan administrator-anggota

> **Note**
>
> Jika Anda menggunakan integrasi CSPM Security Hub denganAWS Organizations, dan belum mengundang akun anggota secara manual, bagian ini tidak berlaku untuk Anda.

Akun tidak dapat berupa akun administrator dan akun anggota secara bersamaan.

Akun anggota hanya dapat dikaitkan dengan satu akun administrator. Jika akun organisasi diaktifkan oleh akun administrator CSPM Security Hub, akun tersebut tidak dapat menerima undangan dari akun lain. Jika akun telah menerima undangan, akun tidak dapat diaktifkan oleh akun administrator CSPM Security Hub untuk organisasi. Itu juga tidak dapat menerima undangan dari akun lain.

Untuk proses undangan manual, menerima undangan keanggotaan adalah opsional.

Keanggotaan melaluiAWS Organizations

Jika Anda mengintegrasikan CSPM Security HubAWS Organizations, akun manajemen Organizations dapat menunjuk akun administrator yang didelegasikan (DA) untuk Security Hub

CSPM. Akun manajemen organisasi tidak dapat ditetapkan sebagai DA di Organizations. Meskipun ini diizinkan di Security Hub CSPM, kami menyarankan agar akun manajemen Organizations tidak boleh menjadi DA.

Kami menyarankan Anda memilih akun DA yang sama di semua Wilayah. Jika Anda menggunakan konfigurasi pusat, maka Security Hub CSPM menetapkan akun DA yang sama di semua Wilayah tempat Anda mengonfigurasi CSPM Security Hub untuk organisasi Anda.

Kami juga menyarankan Anda memilih akun DA yang sama di seluruh layanan AWS keamanan dan kepatuhan untuk membantu Anda mengelola masalah terkait keamanan dalam satu panel kaca.

Keanggotaan berdasarkan undangan

Untuk akun anggota yang dibuat berdasarkan undangan, asosiasi akun administrator-anggota dibuat hanya di Wilayah tempat undangan dikirim. Akun administrator harus mengaktifkan CSPM Security Hub di setiap Wilayah tempat Anda ingin menggunakannya. Akun administrator kemudian mengundang setiap akun untuk menjadi akun anggota di Wilayah tersebut.

> **Note**
>
> Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda.

Mengkoordinasikan akun administrator di seluruh layanan

Security Hub CSPM mengumpulkan temuan dari berbagai AWS layanan, seperti Amazon, Amazon GuardDuty Inspector, dan Amazon Macie. Security Hub CSPM juga memungkinkan pengguna untuk beralih dari GuardDuty temuan untuk memulai penyelidikan di Amazon Detective.

Namun, hubungan administrator-anggota yang Anda atur di layanan lain ini tidak secara otomatis berlaku untuk CSPM Security Hub. Security Hub CSPM merekomendasikan agar Anda menggunakan akun yang sama dengan akun administrator untuk semua layanan ini. Akun administrator ini harus menjadi akun yang bertanggung jawab atas alat keamanan. Akun yang sama juga harus menjadi akun agregator untukAWS Config.

Misalnya, pengguna dari akun GuardDuty administrator A dapat melihat temuan untuk akun GuardDuty anggota B dan C di GuardDuty konsol. Jika akun A kemudian mengaktifkan Security Hub CSPM, pengguna dari akun A tidak secara otomatis melihat GuardDuty temuan untuk akun B dan C

di Security Hub CSPM. Hubungan administrator-anggota CSPM Security Hub juga diperlukan untuk akun-akun ini.

Untuk melakukan ini, jadikan akun A sebagai akun administrator CSPM Security Hub dan aktifkan akun B dan C untuk menjadi akun anggota CSPM Security Hub.

Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations

Anda dapat mengintegrasikan CSPM AWS Security Hub denganAWS Organizations, dan kemudian mengelola Security Hub CSPM untuk akun di organisasi Anda.

Untuk mengintegrasikan CSPM Security Hub denganAWS Organizations, Anda membuat organisasi di. AWS Organizations Akun manajemen Organizations menetapkan satu akun sebagai administrator yang didelegasikan CSPM Security Hub untuk organisasi. Administrator yang didelegasikan kemudian dapat mengaktifkan CSPM Security Hub untuk akun lain di organisasi, menambahkan akun tersebut sebagai akun anggota CSPM Security Hub, dan mengambil tindakan yang diizinkan pada akun anggota. Administrator yang didelegasikan CSPM Security Hub dapat mengaktifkan dan mengelola Security Hub CSPM hingga 10.000 akun anggota.

Tingkat kemampuan konfigurasi administrator yang didelegasikan bergantung pada apakah Anda menggunakan konfigurasi pusat. Dengan konfigurasi pusat diaktifkan, Anda tidak perlu mengonfigurasi CSPM Security Hub secara terpisah di setiap akun anggota dan. Wilayah AWS Administrator yang didelegasikan dapat menerapkan pengaturan CSPM Security Hub tertentu di akun anggota dan unit organisasi (OU) tertentu di seluruh Wilayah.

Akun administrator yang didelegasikan CSPM Security Hub dapat melakukan tindakan berikut pada akun anggota:

- Jika menggunakan konfigurasi pusat, konfigurasikan CSPM Security Hub secara terpusat untuk akun anggota dan OU dengan membuat kebijakan konfigurasi CSPM Security Hub. Kebijakan konfigurasi dapat digunakan untuk mengaktifkan dan menonaktifkan Security Hub CSPM, mengaktifkan dan menonaktifkan standar, serta mengaktifkan dan menonaktifkan kontrol.
- Secara otomatis memperlakukan akun baru sebagai akun anggota CSPM Security Hub ketika mereka bergabung dengan organisasi. Jika Anda menggunakan konfigurasi pusat, kebijakan konfigurasi yang terkait dengan OU mencakup akun yang ada dan baru yang merupakan bagian dari OU.
- Perlakukan akun organisasi yang ada sebagai akun anggota CSPM Security Hub. Ini terjadi secara otomatis jika Anda menggunakan konfigurasi pusat.

- Putuskan akun anggota yang termasuk dalam organisasi. Jika Anda menggunakan konfigurasi pusat, Anda dapat memisahkan akun anggota hanya setelah menetapkannya sebagai dikelola sendiri. Atau, Anda dapat mengaitkan kebijakan konfigurasi yang menonaktifkan CSPM Security Hub dengan akun anggota tertentu yang dikelola secara terpusat.

Jika Anda tidak ikut serta dalam konfigurasi pusat, organisasi Anda menggunakan jenis konfigurasi default yang disebut konfigurasi lokal. Di bawah konfigurasi lokal, administrator yang didelegasikan memiliki kemampuan yang lebih terbatas untuk menerapkan pengaturan di akun anggota. Untuk informasi selengkapnya, lihat Memahami konfigurasi lokal di Security Hub CSPM.

Untuk daftar lengkap tindakan yang dapat dilakukan administrator yang didelegasikan pada akun anggota, lihatTindakan yang diizinkan oleh administrator dan akun anggota di Security Hub CSPM.

Topik di bagian ini menjelaskan cara mengintegrasikan CSPM Security Hub dengan AWS Organizations dan cara mengelola CSPM Security Hub untuk akun dalam suatu organisasi. Jika relevan, setiap bagian mengidentifikasi manfaat dan perbedaan manajemen untuk pengguna konfigurasi pusat.

Topik

- Mengintegrasikan CSPM Security Hub denganAWS Organizations
- Mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru
- Mengaktifkan CSPM Security Hub secara manual di akun organisasi baru
- Memutuskan akun anggota CSPM Security Hub dari organisasi Anda

Mengintegrasikan CSPM Security Hub denganAWS Organizations

Untuk mengintegrasikan CSPM AWS Security Hub danAWS Organizations, Anda membuat organisasi di Organizations dan menggunakan akun manajemen organisasi untuk menunjuk akun administrator CSPM Security Hub yang didelegasikan. Hal ini memungkinkan Security Hub CSPM sebagai layanan terpercaya di Organizations. Ini juga memungkinkan Security Hub CSPM saat ini Wilayah AWS untuk akun administrator yang didelegasikan, dan memungkinkan administrator yang didelegasikan untuk mengaktifkan CSPM Security Hub untuk akun anggota, melihat data di akun anggota, dan melakukan tindakan lain yang diizinkan pada akun anggota.

Jika Anda menggunakan konfigurasi pusat, administrator yang didelegasikan juga dapat membuat kebijakan konfigurasi CSPM Security Hub yang menentukan bagaimana layanan, standar, dan kontrol CSPM Security Hub harus dikonfigurasi di akun organisasi.

Membuat organisasi

Organisasi adalah entitas yang Anda buat untuk mengkonsolidasikan Anda Akun AWS sehingga Anda dapat mengelolanya sebagai satu kesatuan.

Anda dapat membuat organisasi dengan menggunakan AWS Organizations konsol atau dengan menggunakan perintah dari AWS CLI atau salah satu SDK API. Untuk petunjuk mendetail, lihat Membuat organisasi di Panduan AWS Organizations Pengguna.

Anda dapat menggunakan AWS Organizations untuk melihat dan mengelola semua akun dalam organisasi secara terpusat. Sebuah organisasi memiliki satu akun manajemen bersama dengan nol atau lebih akun anggota. Anda dapat mengatur akun dalam struktur hierarkis seperti pohon dengan root di bagian atas dan unit organisasi (OU) bersarang di bawah root. Setiap akun dapat langsung di bawah root, atau ditempatkan di salah satu OU dalam hierarki. OU adalah wadah untuk akun tertentu. Misalnya, Anda dapat membuat OU keuangan yang mencakup semua akun yang terkait dengan operasi keuangan.

Rekomendasi untuk memilih administrator CSPM Security Hub yang didelegasikan

Jika Anda memiliki akun administrator dari proses undangan manual dan sedang beralih ke manajemen akunAWS Organizations, sebaiknya tentukan akun tersebut sebagai administrator CSPM Security Hub yang didelegasikan.

Meskipun API dan konsol CSPM Security Hub memungkinkan akun manajemen organisasi menjadi administrator CSPM Security Hub yang didelegasikan, sebaiknya pilih dua akun yang berbeda. Ini karena pengguna yang memiliki akses ke akun manajemen organisasi untuk mengelola penagihan cenderung berbeda dari pengguna yang membutuhkan akses ke Security Hub CSPM untuk manajemen keamanan.

Sebaiknya gunakan administrator yang didelegasikan sama di seluruh Wilayah. Jika Anda ikut serta dalam konfigurasi pusat, Security Hub CSPM secara otomatis menunjuk administrator yang didelegasikan yang sama di Wilayah asal Anda dan Wilayah yang ditautkan.

Verifikasi izin untuk mengonfigurasi administrator yang didelegasikan

Untuk menetapkan dan menghapus akun administrator CSPM Security Hub yang didelegasikan, akun manajemen organisasi harus memiliki izin dan tindakan `EnableOrganizationAdminAccount` di CSPM `DisableOrganizationAdminAccount` Security Hub. Akun manajemen Organizations juga harus memiliki izin administratif untuk Organizations.

Untuk memberikan semua izin yang diperlukan, lampirkan kebijakan terkelola CSPM Security Hub berikut ke kepala IAM untuk akun manajemen organisasi:

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

Menunjuk administrator yang didelegasikan

Untuk menetapkan akun administrator CSPM Security Hub yang didelegasikan, Anda dapat menggunakan konsol CSPM Security Hub, Security Hub CSPM API, atau. AWS CLI Security Hub CSPM menetapkan administrator yang didelegasikan Wilayah AWS hanya di saat ini, dan Anda harus mengulangi tindakan di Wilayah lain. Jika Anda mulai menggunakan konfigurasi pusat, maka Security Hub CSPM secara otomatis menetapkan administrator yang didelegasikan yang sama di Wilayah beranda dan Wilayah yang ditautkan.

Akun manajemen organisasi tidak harus mengaktifkan CSPM Security Hub untuk menetapkan akun administrator CSPM Security Hub yang didelegasikan.

Kami menyarankan agar akun manajemen organisasi bukan akun administrator CSPM Security Hub yang didelegasikan. Namun, jika Anda memilih akun manajemen organisasi sebagai administrator yang didelegasikan CSPM Security Hub, akun manajemen harus mengaktifkan CSPM Security Hub. Jika akun manajemen tidak mengaktifkan Security Hub CSPM, Anda harus mengaktifkan Security Hub CSPM untuk itu secara manual. CSPM Security Hub tidak dapat diaktifkan secara otomatis untuk akun manajemen organisasi.

Anda harus menunjuk administrator CSPM Security Hub yang didelegasikan menggunakan salah satu metode berikut. Menunjuk administrator CSPM Security Hub yang didelegasikan dengan Organizations API tidak tercermin dalam Security Hub CSPM.

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah untuk menetapkan akun administrator CSPM Security Hub yang didelegasikan.

Security Hub CSPM console

Untuk menunjuk administrator yang didelegasikan saat melakukan orientasi

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Buka Security Hub CSPM. Anda diminta untuk masuk ke akun manajemen organisasi.

3. Pada halaman Tentukan administrator yang didelegasikan, di bagian Akun administrator yang didelegasikan, tentukan akun administrator yang didelegasikan. Sebaiknya pilih administrator yang didelegasikan sama yang telah Anda tetapkan untuk layanan AWS keamanan dan kepatuhan lainnya.
4. Pilih Setel administrator yang didelegasikan. Anda diminta untuk masuk ke akun administrator yang didelegasikan (jika belum) untuk melanjutkan orientasi dengan konfigurasi pusat. Jika Anda tidak ingin memulai konfigurasi pusat, pilih Batal. Administrator yang didelegasikan Anda disetel, tetapi Anda belum menggunakan konfigurasi pusat.

Untuk menunjuk administrator yang didelegasikan dari Pengaturan halaman

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi CSPM Security Hub, pilih Pengaturan. Kemudian pilih Umum.
3. Jika akun administrator CSPM Security Hub saat ini ditetapkan, maka sebelum Anda dapat menunjuk akun baru, Anda harus menghapus akun saat ini.

   Di bawah Administrator Delegasi, untuk menghapus akun saat ini, pilih Hapus.
4. Masukkan ID akun akun yang ingin Anda tetapkan sebagai akun administrator CSPM Security Hub.

   Anda harus menetapkan akun administrator CSPM Security Hub yang sama di semua Wilayah. Jika Anda menetapkan akun yang berbeda dari akun yang ditunjuk di Wilayah lain, konsol mengembalikan kesalahan.
5. Pilih Delegasikan.

Security Hub CSPM API,AWS CLI

Dari akun manajemen organisasi, gunakan EnableOrganizationAdminAccountpengoperasian Security Hub CSPM API. Jika Anda menggunakanAWS CLI, jalankan enable-organization-admin-accountperintah. Berikan Akun AWS ID administrator CSPM Security Hub yang didelegasikan.

Contoh berikut menunjuk administrator CSPM Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

Menghapus atau mengubah administrator yang didelegasikan

Hanya akun manajemen organisasi yang dapat menghapus akun administrator CSPM Security Hub yang didelegasikan.

Untuk mengubah administrator CSPM Security Hub yang didelegasikan, Anda harus terlebih dahulu menghapus akun administrator yang didelegasikan saat ini dan kemudian menunjuk yang baru.

> **Warning**
>
> Bila Anda menggunakan konfigurasi pusat, Anda tidak dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API untuk mengubah atau menghapus akun administrator yang didelegasikan. Jika akun manajemen organisasi menggunakan AWS Organizations konsol atau AWS Organizations API untuk mengubah atau menghapus administrator CSPM Security Hub yang didelegasikan, CSPM Security Hub secara otomatis menghentikan konfigurasi pusat, dan menghapus kebijakan konfigurasi dan asosiasi kebijakan Anda. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus.

Jika Anda menggunakan konsol CSPM Security Hub untuk menghapus administrator yang didelegasikan di satu Wilayah, maka secara otomatis dihapus di semua Wilayah.

Security Hub CSPM API hanya menghapus akun administrator CSPM Security Hub yang didelegasikan dari Wilayah tempat panggilan API atau perintah dikeluarkan. Anda harus mengulangi tindakan di Wilayah lain.

Jika Anda menggunakan Organizations API untuk menghapus akun administrator CSPM Security Hub yang didelegasikan, akun tersebut akan dihapus secara otomatis di semua Wilayah.

Menghapus administrator yang didelegasikan (Organizations API,AWS CLI)

Anda dapat menggunakan Organizations untuk menghapus administrator CSPM Security Hub yang didelegasikan di semua Wilayah.

Jika Anda menggunakan konfigurasi pusat untuk mengelola akun, menghapus akun administrator yang didelegasikan akan mengakibatkan penghapusan kebijakan konfigurasi dan asosiasi kebijakan Anda. Akun anggota mempertahankan konfigurasi yang mereka miliki sebelum administrator yang didelegasikan diubah atau dihapus. Namun, akun ini tidak dapat dikelola lagi oleh akun

administrator yang didelegasikan yang dihapus. Mereka menjadi akun yang dikelola sendiri yang harus dikonfigurasi secara terpisah di setiap Wilayah.

Pilih metode yang Anda inginkan, dan ikuti petunjuk untuk menghapus akun administrator CSPM Security Hub yang didelegasikan. AWS Organizations

Organizations API,AWS CLI

Untuk menghapus administrator CSPM Security Hub yang didelegasikan

Dari akun manajemen organisasi, gunakan DeregisterDelegatedAdministratorpengoperasian API Organizations. Jika Anda menggunakanAWS CLI, jalankan perintah deregister-delegated-administrator. Berikan ID akun administrator yang didelegasikan, dan kepala layanan untuk Security Hub CSPM, yaitu. `securityhub.amazonaws.com`

Contoh berikut menghapus administrator CSPM Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Menghapus administrator yang didelegasikan (konsol CSPM Security Hub)

Anda dapat menggunakan konsol CSPM Security Hub untuk menghapus administrator CSPM Security Hub yang didelegasikan di semua Wilayah.

Ketika akun administrator CSPM Security Hub yang didelegasikan dihapus, akun anggota akan dipisahkan dari akun administrator CSPM Security Hub yang didelegasikan yang dihapus.

Security Hub CSPM masih diaktifkan di akun anggota. Mereka menjadi akun mandiri sampai administrator CSPM Security Hub baru memungkinkan mereka sebagai akun anggota.

Jika akun manajemen organisasi bukan akun yang diaktifkan di CSPM Security Hub, gunakan opsi di halaman CSPM Selamat Datang di Security Hub.

Untuk menghapus akun administrator CSPM Security Hub yang didelegasikan dari Selamat datang di Security Hub CSPM halaman

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

2. Pilih Buka Security Hub.
3. Di bawah Administrator Delegasi, pilih Hapus.

Jika akun manajemen organisasi adalah akun yang diaktifkan di Security Hub, maka gunakan opsi pada tab Umum pada halaman Pengaturan.

Untuk menghapus akun administrator CSPM Security Hub yang didelegasikan dari Pengaturan halaman

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi CSPM Security Hub, pilih Pengaturan. Kemudian pilih Umum.
3. Di bawah Administrator Delegasi, pilih Hapus.

Menghapus administrator yang didelegasikan (Security Hub CSPM API,AWS CLI)

Anda dapat menggunakan Security Hub CSPM API atau operasi CSPM Security Hub AWS CLI untuk menghapus administrator CSPM Security Hub yang didelegasikan. Saat Anda menghapus administrator yang didelegasikan dengan salah satu metode ini, administrator hanya akan dihapus di Wilayah tempat panggilan atau perintah API dikeluarkan. Security Hub CSPM tidak memperbarui Wilayah lain, dan tidak menghapus akun administrator yang didelegasikan. AWS Organizations

Pilih metode yang Anda inginkan, dan ikuti langkah-langkah berikut untuk menghapus akun administrator CSPM Security Hub yang didelegasikan dengan Security Hub CSPM.

Security Hub CSPM API,AWS CLI

Untuk menghapus administrator CSPM Security Hub yang didelegasikan

Dari akun manajemen organisasi, gunakan DisableOrganizationAdminAccountpengoperasian Security Hub CSPM API. Jika Anda menggunakanAWS CLI, jalankan disable-organization-admin-accountperintah. Berikan ID akun administrator CSPM Security Hub yang didelegasikan.

Contoh berikut menghapus administrator CSPM Security Hub yang didelegasikan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Menonaktifkan integrasi CSPM Security Hub denganAWS Organizations

Setelah AWS Organizations organisasi terintegrasi dengan AWS Security Hub CSPM, akun manajemen Organizations selanjutnya dapat menonaktifkan integrasi. Sebagai pengguna akun manajemen Organizations, Anda dapat melakukannya dengan menonaktifkan akses tepercaya untuk Security Hub CSPM di. AWS Organizations

Ketika Anda menonaktifkan akses tepercaya untuk Security Hub CSPM, hal berikut akan terjadi:

- Security Hub CSPM kehilangan statusnya sebagai layanan tepercaya di. AWS Organizations
- Akun administrator yang didelegasikan CSPM Security Hub kehilangan akses ke pengaturan, data, dan sumber daya CSPM Security Hub untuk semua akun anggota CSPM Security Hub secara keseluruhan. Wilayah AWS
- Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis berhenti menggunakannya untuk organisasi Anda. Kebijakan konfigurasi dan asosiasi kebijakan Anda dihapus. Akun mempertahankan konfigurasi yang mereka miliki sebelum Anda menonaktifkan akses tepercaya.
- Semua akun anggota CSPM Security Hub menjadi akun mandiri dan mempertahankan pengaturan mereka saat ini. Jika Security Hub CSPM diaktifkan untuk akun anggota di satu atau beberapa Wilayah, CSPM Security Hub tetap diaktifkan untuk akun di Wilayah tersebut. Standar dan kontrol yang diaktifkan juga tidak berubah. Anda dapat mengubah pengaturan ini secara terpisah di setiap akun dan Wilayah. Namun, akun tidak lagi dikaitkan dengan administrator yang didelegasikan di Wilayah mana pun.

Untuk informasi tambahan tentang hasil menonaktifkan akses layanan tepercaya, lihat Menggunakan AWS Organizations dengan yang lain Layanan AWS di AWS OrganizationsPanduan Pengguna.

Untuk menonaktifkan akses tepercaya, Anda dapat menggunakan AWS Organizations konsol, Organizations API, atau fileAWS CLI. Hanya pengguna akun manajemen Organizations yang dapat menonaktifkan akses layanan tepercaya untuk Security Hub CSPM. Untuk detail tentang izin yang Anda perlukan, lihat Izin yang diperlukan untuk menonaktifkan akses tepercaya di AWS OrganizationsPanduan Pengguna.

Sebelum Anda menonaktifkan akses tepercaya, kami sarankan bekerja sama dengan administrator yang didelegasikan untuk organisasi Anda untuk menonaktifkan CSPM Security Hub di akun anggota dan membersihkan sumber daya CSPM Security Hub di akun tersebut.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menonaktifkan akses tepercaya untuk Security Hub CSPM.

Organizations console

Untuk menonaktifkan akses tepercaya untuk Security Hub CSPM

1. Masuk ke Konsol Manajemen AWS menggunakan kredensyal akun AWS Organizations manajemen.
2. Buka konsol Organizations di https://console.aws.amazon.com/organizations/.
3. Pada panel navigasi, silakan pilih Layanan.
4. Di bawah Layanan terintegrasi, pilih AWSSecurity Hub CSPM.
5. Pilih Menonaktifkan akses terpercaya.
6. Konfirmasikan bahwa Anda ingin menonaktifkan akses tepercaya.

Organizations API

Untuk menonaktifkan akses tepercaya untuk Security Hub CSPM

Memanggil DisableAWSServiceAccessoperasi AWS Organizations API. Untuk `ServicePrincipal` parameternya, tentukan prinsip layanan CSPM Security Hub ()`securityhub.amazonaws.com`.

AWS CLI

Untuk menonaktifkan akses tepercaya untuk Security Hub CSPM

Jalankan perintah disable-aws-service-access dari API. AWS Organizations Untuk `service-principal` parameternya, tentukan prinsip layanan CSPM Security Hub ()`securityhub.amazonaws.com`.

Contoh:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

Mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru

Saat akun baru bergabung dengan organisasi Anda, akun tersebut akan ditambahkan ke daftar di halaman Akun konsol CSPM AWS Security Hub. Untuk akun organisasi, Type is By Organization. Secara default, akun baru tidak menjadi anggota CSPM Security Hub saat mereka bergabung dengan organisasi. Status mereka bukan anggota. Akun administrator yang didelegasikan dapat secara otomatis menambahkan akun baru sebagai anggota dan mengaktifkan CSPM Security Hub di akun ini saat mereka bergabung dengan organisasi.

> **Note**
>
> Meskipun banyak Wilayah AWS yang aktif secara default untuk AndaAkun AWS, Anda harus mengaktifkan Wilayah tertentu secara manual. Wilayah ini disebut Wilayah keikutsertaan dalam dokumen ini. Untuk mengaktifkan CSPM Security Hub secara otomatis di akun baru di Region opt-in, akun tersebut harus mengaktifkan Region tersebut terlebih dahulu. Hanya pemilik akun yang dapat mengaktifkan Wilayah keikutsertaan. Untuk informasi selengkapnya tentang opt-in Regions, lihat Menentukan yang dapat digunakan akun Wilayah AWS Anda.

Proses ini berbeda berdasarkan apakah Anda menggunakan konfigurasi pusat (disarankan) atau konfigurasi lokal.

Mengaktifkan akun organisasi baru secara otomatis (konfigurasi pusat)

Jika Anda menggunakan konfigurasi pusat, Anda dapat mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru dan yang sudah ada dengan membuat kebijakan konfigurasi tempat CSPM Security Hub diaktifkan. Anda kemudian dapat mengaitkan kebijakan dengan root organisasi atau unit organisasi tertentu (OU).

Jika Anda mengaitkan kebijakan konfigurasi di mana Security Hub CSPM diaktifkan dengan OU tertentu, Security Hub CSPM secara otomatis diaktifkan di semua akun (yang ada dan baru) milik OU tersebut. Akun baru yang bukan milik OU dikelola sendiri dan tidak secara otomatis mengaktifkan Security Hub CSPM. Jika Anda mengaitkan kebijakan konfigurasi di mana Security Hub CSPM diaktifkan dengan root, Security Hub CSPM secara otomatis diaktifkan di semua akun (yang ada dan baru) yang bergabung dengan organisasi. Pengecualian adalah jika akun menggunakan kebijakan yang berbeda melalui aplikasi atau warisan, atau dikelola sendiri.

Dalam kebijakan konfigurasi, Anda juga dapat menentukan standar dan kontrol keamanan mana yang harus diaktifkan di OU. Untuk menghasilkan temuan kontrol untuk standar yang diaktifkan,

akun di OU harus AWS Config diaktifkan dan dikonfigurasi untuk mencatat sumber daya yang diperlukan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Untuk petunjuk cara membuat kebijakan konfigurasi, lihatMembuat dan mengaitkan kebijakan konfigurasi.

Mengaktifkan akun organisasi baru secara otomatis (konfigurasi lokal)

Saat Anda menggunakan konfigurasi lokal dan mengaktifkan pengaktifan otomatis standar default, Security Hub CSPM menambahkan akun organisasi baru sebagai anggota dan mengaktifkan CSPM Security Hub di dalamnya di Wilayah saat ini. Wilayah lain tidak terpengaruh. Selain itu, mengaktifkan pengaktifan otomatis tidak mengaktifkan CSPM Security Hub di akun organisasi yang ada kecuali akun tersebut sudah ditambahkan sebagai akun anggota.

Setelah mengaktifkan pengaktifan otomatis, standar keamanan default diaktifkan untuk akun anggota baru di Wilayah saat ini ketika mereka bergabung dengan organisasi. Standar default adalah AWS Foundational Security Best Practices (FSBP) dan Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0. Anda tidak dapat mengubah standar default. Jika Anda ingin mengaktifkan standar lain di seluruh organisasi Anda, atau mengaktifkan standar untuk akun dan OU tertentu, sebaiknya gunakan konfigurasi pusat.

Untuk menghasilkan temuan kontrol untuk standar default (dan standar lain yang diaktifkan), akun di organisasi Anda harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan. Untuk informasi selengkapnya tentang AWS Config perekaman, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru. Petunjuk ini hanya berlaku jika Anda menggunakan konfigurasi lokal.

Security Hub CSPM console

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota CSPM Security Hub

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Tanda menggunakan kredensi akun administrator yang didelegasikan.
2. Di panel navigasi CSPM Security Hub, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, nyalakan Auto-enable akun.

Security Hub CSPM API

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota CSPM Security Hub

Memanggil `UpdateOrganizationConfiguration`API dari akun administrator yang didelegasikan. Setel `AutoEnable` bidang `true` untuk mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru.

AWS CLI

Untuk mengaktifkan akun organisasi baru secara otomatis sebagai anggota CSPM Security Hub

Jalankan `update-organization-configuration`perintah dari akun administrator yang didelegasikan. Sertakan `auto-enable` parameter untuk mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru.

```
aws securityhub update-organization-configuration --auto-enable
```

Mengaktifkan CSPM Security Hub secara manual di akun organisasi baru

Jika Anda tidak mengaktifkan CSPM Security Hub secara otomatis di akun organisasi baru saat mereka bergabung dengan organisasi, Anda dapat menambahkan akun tersebut sebagai anggota dan mengaktifkan CSPM Security Hub di dalamnya secara manual setelah mereka bergabung dengan organisasi. Anda juga harus mengaktifkan CSPM Security Hub secara manual Akun AWS karena sebelumnya Anda terputus dari organisasi.

> **Note**
>
> Bagian ini tidak berlaku untuk Anda jika Anda menggunakan konfigurasi pusat. Jika Anda menggunakan konfigurasi pusat, Anda dapat membuat kebijakan konfigurasi yang mengaktifkan CSPM Security Hub di akun anggota tertentu dan unit organisasi (OU). Anda juga dapat mengaktifkan standar dan kontrol tertentu di akun dan OU tersebut.

Anda tidak dapat mengaktifkan CSPM Security Hub di akun jika sudah menjadi akun anggota dalam organisasi yang berbeda.

Anda juga tidak dapat mengaktifkan CSPM Security Hub di akun yang saat ini ditangguhkan. Jika Anda mencoba mengaktifkan layanan di akun yang ditangguhkan, status akun berubah menjadi Akun Ditangguhkan.

- Jika akun tidak mengaktifkan CSPM Security Hub, CSPM Security Hub diaktifkan di akun tersebut. Standar AWS Foundational Security Best Practices (FSBP) dan CIS AWS Foundations Benchmark v1.2.0 juga diaktifkan di akun kecuali Anda mematikan standar keamanan default.

  Pengecualian untuk ini adalah akun manajemen Organizations. Security Hub CSPM tidak dapat diaktifkan secara otomatis di akun manajemen Organisasi. Anda harus mengaktifkan CSPM Security Hub secara manual di akun manajemen Organisasi sebelum dapat menambahkannya sebagai akun anggota.
- Jika akun sudah mengaktifkan Security Hub CSPM, Security Hub CSPM tidak membuat perubahan lain pada akun tersebut. Ini hanya memungkinkan keanggotaan.

Agar Security Hub CSPM dapat menghasilkan temuan kontrol, akun anggota harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam sumber daya yang diperlukan. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan akun organisasi sebagai akun anggota CSPM Security Hub.

Security Hub CSPM console

Mengaktifkan akun organisasi secara manual sebagai anggota CSPM Security Hub

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator yang didelegasikan.
2. Di panel navigasi CSPM Security Hub, di bawah Pengaturan, pilih Konfigurasi.
3. Dalam daftar Akun, pilih setiap akun organisasi yang ingin Anda aktifkan.
4. Pilih Tindakan, lalu pilih Tambah anggota.

Security Hub CSPM API

Mengaktifkan akun organisasi secara manual sebagai anggota CSPM Security Hub

Memanggil `CreateMembers`API dari akun administrator yang didelegasikan. Agar setiap akun dapat diaktifkan, berikan ID akun.

Tidak seperti proses undangan manual, ketika Anda memanggil `CreateMembers` untuk mengaktifkan akun organisasi, Anda tidak perlu mengirim undangan.

AWS CLI

Mengaktifkan akun organisasi secara manual sebagai anggota CSPM Security Hub

Jalankan `create-members`perintah dari akun administrator yang didelegasikan. Agar setiap akun dapat diaktifkan, berikan ID akun.

Berbeda dengan proses undangan manual, ketika Anda menjalankan `create-members` untuk mengaktifkan akun organisasi, Anda tidak perlu mengirim undangan.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Contoh

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Memutuskan akun anggota CSPM Security Hub dari organisasi Anda

Untuk berhenti menerima dan melihat temuan dari akun anggota CSPM AWS Security Hub, Anda dapat memisahkan akun anggota dari organisasi Anda.

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, disasosiasi bekerja secara berbeda. Anda dapat membuat kebijakan konfigurasi yang menonaktifkan CSPM Security Hub di satu atau beberapa akun anggota yang dikelola secara terpusat. Setelah itu, akun-akun ini masih menjadi bagian dari organisasi, tetapi tidak akan menghasilkan temuan CSPM Security Hub. Jika Anda menggunakan konfigurasi pusat tetapi juga memiliki akun anggota yang diundang secara manual, Anda dapat memisahkan satu atau beberapa akun yang diundang secara manual.

Akun anggota yang dikelola menggunakan tidak AWS Organizations dapat memisahkan akun mereka dari akun administrator. Hanya akun administrator yang dapat memisahkan akun anggota.

Memutuskan hubungan akun anggota tidak menutup akun. Sebaliknya, itu menghapus akun anggota dari organisasi. Akun anggota yang terputus menjadi mandiri Akun AWS yang tidak lagi dikelola oleh integrasi CSPM Security Hub dengan. AWS Organizations

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun anggota dari organisasi.

Security Hub CSPM console

Untuk memisahkan akun anggota dari organisasi

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator yang didelegasikan.
2. Di panel navigasi, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, pilih akun yang ingin Anda pisahkan. Jika Anda menggunakan konfigurasi pusat, Anda dapat memilih akun yang diundang secara manual untuk dipisahkan dari tab. `Invitation accounts` Tab ini hanya terlihat jika Anda menggunakan konfigurasi pusat.
4. Pilih Tindakan, lalu pilih Putuskan akun.

Security Hub CSPM API

Untuk memisahkan akun anggota dari organisasi

Memanggil `DisassociateMembers`API dari akun administrator yang didelegasikan. Anda harus memberikan Akun AWS ID untuk akun anggota untuk dipisahkan. Untuk melihat daftar akun anggota, panggil `ListMembers`API.

AWS CLI

Untuk memisahkan akun anggota dari organisasi

Jalankan `disassociate-membersperintah>` dari akun administrator yang didelegasikan. Anda harus memberikan Akun AWS ID untuk akun anggota untuk dipisahkan. Untuk melihat daftar akun anggota, jalankan `list-membersperintah>`.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Contoh

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Anda juga dapat menggunakan AWS Organizations konsol,AWS CLI, atau AWS SDK untuk memisahkan akun anggota dari organisasi Anda. Untuk informasi selengkapnya, lihat Menghapus akun anggota dari organisasi Anda di Panduan AWS Organizations Pengguna.

Mengelola akun dengan undangan di Security Hub CSPM

Anda dapat mengelola beberapa akun CSPM AWS Security Hub secara terpusat dengan dua cara, dengan mengintegrasikan Security Hub CSPM AWS Organizations dengan atau dengan mengirim dan menerima undangan keanggotaan secara manual. Anda harus menggunakan proses manual jika Anda memiliki akun mandiri atau Anda tidak berintegrasi dengannyaAWS Organizations. Dalam manajemen akun manual, administrator CSPM Security Hub mengundang akun untuk menjadi anggota. Hubungan administrator-anggota terjalin ketika calon anggota menerima undangan. Akun administrator CSPM Security Hub dapat mengelola CSPM Security Hub hingga 1.000 akun anggota berbasis undangan.

> **Note**
>
> Jika Anda membuat organisasi berbasis undangan di Security Hub CSPM, Anda selanjutnya dapat beralih menggunakan. AWS Organizations Jika Anda memiliki lebih dari satu akun anggota, sebaiknya AWS Organizations gunakan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations.

Cross-Region agregasi temuan dan data lainnya tersedia untuk akun yang Anda undang melalui proses undangan manual. Namun, administrator harus mengundang akun anggota dari Wilayah agregasi dan semua Wilayah yang ditautkan agar agregasi lintas wilayah berfungsi. Selain itu, akun anggota harus mengaktifkan CSPM Security Hub di Wilayah agregasi dan semua Wilayah yang ditautkan untuk memberikan administrator kemampuan untuk melihat temuan dari akun anggota.

Kebijakan konfigurasi tidak didukung untuk akun anggota yang diundang secara manual. Sebagai gantinya, Anda harus mengonfigurasi pengaturan CSPM Security Hub secara terpisah di setiap akun anggota dan Wilayah AWS saat Anda menggunakan proses undangan manual.

Anda juga harus menggunakan proses berbasis undangan manual untuk akun yang bukan milik organisasi Anda. Misalnya, Anda mungkin tidak menyertakan akun pengujian di organisasi Anda. Atau, Anda mungkin ingin menggabungkan akun dari beberapa organisasi di bawah satu akun administrator CSPM Security Hub. Akun administrator CSPM Security Hub harus mengirim undangan ke akun milik organisasi lain.

Pada halaman Konfigurasi konsol CSPM Security Hub, akun yang ditambahkan melalui undangan tercantum di tab Akun undangan. Jika Anda menggunakan konfigurasi pusat, tetapi juga mengundang akun di luar organisasi, Anda dapat melihat temuan dari akun berbasis undangan di tab ini. Namun, administrator CSPM Security Hub tidak dapat mengonfigurasi akun berbasis undangan di seluruh Wilayah melalui penggunaan kebijakan konfigurasi.

Topik di bagian ini menjelaskan cara mengelola akun anggota melalui undangan.

Topik

- Menambahkan dan mengundang akun anggota di Security Hub CSPM
- Menanggapi undangan untuk menjadi akun anggota CSPM Security Hub
- Memutuskan akun anggota di Security Hub CSPM
- Menghapus akun anggota di Security Hub CSPM
- Memutuskan hubungan dari akun administrator CSPM Security Hub
- Transisi ke Organizations untuk mengelola akun di Security Hub CSPM

Menambahkan dan mengundang akun anggota di Security Hub CSPM

> **Note**
>
> Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations.

Akun Anda menjadi administrator CSPM AWS Security Hub untuk akun yang menerima undangan Anda untuk menjadi akun anggota CSPM Security Hub.

Ketika Anda menerima undangan dari akun lain, akun Anda menjadi akun anggota, dan akun itu menjadi administrator Anda.

Jika akun Anda adalah akun administrator, Anda tidak dapat menerima undangan untuk menjadi akun anggota.

Menambahkan akun anggota terdiri dari langkah-langkah berikut:

1. Akun administrator menambahkan akun anggota ke daftar akun anggota mereka.

2. Akun administrator mengirimkan undangan ke akun anggota.
3. Akun anggota menerima undangan.

Menambahkan akun anggota

Dari konsol CSPM Security Hub, Anda dapat menambahkan akun ke daftar akun anggota Anda. Di konsol CSPM Security Hub, Anda dapat memilih akun satu per satu, atau mengunggah `.csv` file yang berisi informasi akun.

Untuk setiap akun, Anda harus memberikan ID akun dan alamat email. Alamat email harus berupa alamat email untuk dihubungi tentang masalah keamanan di akun. Ini tidak digunakan untuk memverifikasi akun.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menambahkan akun anggota.

Security Hub CSPM console

Untuk menambahkan akun ke daftar akun anggota

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator.
2. Di panel kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih Akun, lalu pilih Tambah akun. Anda kemudian dapat menambahkan akun satu per satu atau mengunggah `.csv` file yang berisi daftar akun.
4. Untuk memilih akun, lakukan salah satu hal berikut:

   - Untuk menambahkan akun satu per satu, di bawah Masukkan akun, masukkan ID akun dan alamat email akun yang akan ditambahkan, lalu pilih Tambah.

     Ulangi proses ini untuk setiap akun.
   - Untuk menggunakan file nilai yang dipisahkan koma (.csv) untuk menambahkan beberapa akun, buat file terlebih dahulu. File harus berisi ID akun dan alamat email untuk ditambahkan setiap akun.

     Dalam `.csv` daftar Anda, akun harus muncul satu per baris. Baris pertama `.csv` file harus berisi header. Di header, kolom pertama adalah **`Account ID`** dan kolom kedua adalah**`Email`**.

Setiap baris berikutnya harus berisi ID akun dan alamat email yang valid untuk ditambahkan akun.

Berikut adalah contoh `.csv` file ketika dilihat di editor teks.

```
Account ID,Email
111111111111,user@example.com
```

Dalam program spreadsheet, bidang muncul di kolom terpisah. Format yang mendasarinya masih dipisahkan koma. Anda harus memformat ID akun sebagai angka non-desimal. Misalnya, ID akun 444455556666 tidak dapat diformat sebagai 444455556666.0. Pastikan juga bahwa pemformatan angka tidak menghapus nol di depan dari ID akun.

Untuk memilih file, di konsol, pilih Unggah daftar (.csv). Kemudian pilih Browse.

Setelah Anda memilih file, pilih Tambah akun.

5. Setelah Anda selesai menambahkan akun, di bawah Akun yang akan ditambahkan, pilih Berikutnya.

Security Hub CSPM API

Untuk menambahkan akun ke daftar akun anggota

Memanggil `CreateMembers`API dari akun administrator. Untuk setiap akun anggota untuk ditambahkan, Anda harus memberikan Akun AWS ID.

AWS CLI

Untuk menambahkan akun ke daftar akun anggota Anda

Jalankan `create-members`perintah dari akun administrator. Untuk setiap akun anggota untuk ditambahkan, Anda harus memberikan Akun AWS ID.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Contoh

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

Mengundang akun anggota

Setelah Anda menambahkan akun anggota, Anda mengirim undangan ke akun anggota. Anda juga dapat mengirim ulang undangan ke akun yang Anda lepaskan dari administrator.

Security Hub CSPM console

Mengundang akun calon member

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator.
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Untuk akun yang akan diundang, pilih Undang di kolom Status.
4. Saat diminta untuk mengonfirmasi, pilih Undang.

> **Note**
>
> Untuk mengirim ulang undangan ke akun yang tidak terkait, pilih setiap akun yang tidak terkait di halaman Akun. Untuk Tindakan, pilih Kirim ulang undangan.

Security Hub CSPM API

Mengundang akun calon member

Memanggil `InviteMembers`API dari akun administrator. Untuk setiap akun yang akan diundang, Anda harus memberikan Akun AWS ID.

AWS CLI

Mengundang akun calon member

Jalankan `invite-members`perintah dari akun administrator. Untuk setiap akun yang akan diundang, Anda harus memberikan Akun AWS ID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Contoh

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Menanggapi undangan untuk menjadi akun anggota CSPM Security Hub

> **Note**
>
> Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations.

Anda dapat menerima atau menolak undangan untuk menjadi akun anggota CSPM AWS Security Hub.

Jika Anda menerima undangan, akun Anda menjadi akun anggota CSPM Security Hub. Akun yang mengirim undangan menjadi akun administrator CSPM Security Hub Anda. Pengguna akun administrator dapat melihat temuan untuk akun anggota Anda di Security Hub CSPM.

Jika Anda menolak undangan, maka akun Anda ditandai sebagai Mengundurkan diri pada daftar akun anggota akun administrator.

Anda hanya dapat menerima satu undangan untuk menjadi akun anggota.

Sebelum Anda dapat menerima atau menolak undangan, Anda harus mengaktifkan Security Hub CSPM.

Ingat bahwa semua akun CSPM Security Hub harus telah AWS Config diaktifkan dan dikonfigurasi untuk merekam semua sumber daya. Untuk detail tentang persyaratanAWS Config, lihat Mengaktifkan dan mengonfigurasi AWS Config.

Menerima undangan

Anda dapat mengirim undangan untuk menjadi akun anggota CSPM Security Hub dari akun administrator. Anda kemudian dapat menerima undangan setelah masuk ke akun anggota.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menerima undangan untuk menjadi akun anggota.

Security Hub CSPM console

Untuk menerima undangan keanggotaan

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, aktifkan Terima, lalu pilih Terima undangan.

Security Hub CSPM API

Untuk menerima undangan keanggotaan

Memanggil `AcceptAdministratorInvitation`API. Anda harus memberikan pengenal undangan dan Akun AWS ID akun administrator. Untuk mengambil detail tentang undangan, gunakan `ListInvitations`operasi.

AWS CLI

Untuk menerima undangan keanggotaan

Jalankan perintah `accept-administrator-invitation`. Anda harus memberikan pengenal undangan dan Akun AWS ID akun administrator. Untuk mengambil detail tentang undangan, jalankan `list-invitations`perintah.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

Contoh

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Konsol CSPM Security Hub terus digunakan. `AcceptInvitation` Ini pada akhirnya akan berubah untuk digunakan`AcceptAdministratorInvitation`. Setiap kebijakan IAM yang secara khusus mengontrol akses ke fungsi ini harus terus digunakan`AcceptInvitation`. Anda juga harus menambahkan kebijakan Anda `AcceptAdministratorInvitation`

untuk memastikan bahwa izin yang benar diberlakukan setelah konsol mulai digunakan`AcceptAdministratorInvitation`.

Menolak undangan

Anda dapat menolak undangan untuk menjadi akun anggota CSPM Security Hub. Saat Anda menolak undangan di konsol CSPM Security Hub, akun Anda ditandai sebagai Mengundurkan diri pada daftar akun anggota akun administrator. Status mengundurkan diri hanya muncul saat Anda masuk ke konsol CSPM Security Hub menggunakan akun administrator. Namun, undangan tetap tidak berubah di konsol untuk akun anggota sampai Anda masuk ke akun administrator dan menghapus undangan.

Untuk menolak undangan, Anda harus masuk ke akun anggota yang menerima undangan.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menolak undangan menjadi akun anggota.

Security Hub CSPM console

Untuk menolak undangan keanggotaan

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, pilih Tolak undangan.

Security Hub CSPM API

Untuk menolak undangan keanggotaan

Memanggil `DeclineInvitations`API. Anda harus memberikan Akun AWS ID akun administrator yang mengeluarkan undangan. Untuk melihat informasi tentang undangan Anda, gunakan operasi. `ListInvitations`

AWS CLI

Untuk menolak undangan keanggotaan

Jalankan perintah `decline-invitations`. Anda harus memberikan Akun AWS ID akun administrator yang mengeluarkan undangan. Untuk melihat informasi tentang undangan Anda, jalankan perintah. `list-invitations`

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Contoh

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Memutuskan akun anggota di Security Hub CSPM

> **Note**
>
> Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations.

Akun administrator CSPM AWS Security Hub dapat memisahkan akun anggota untuk berhenti menerima dan melihat temuan dari akun tersebut. Anda harus memisahkan akun anggota sebelum Anda dapat menghapusnya.

Saat Anda memisahkan akun anggota, akun tersebut tetap ada dalam daftar akun anggota Anda dengan status Dihapus (Terputus). Akun Anda dihapus dari informasi akun administrator untuk akun anggota.

Untuk melanjutkan menerima temuan untuk akun, Anda dapat mengirim ulang undangan. Untuk menghapus akun anggota sepenuhnya, Anda dapat menghapus akun anggota.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk memisahkan akun anggota yang diundang secara manual dari akun administrator.

Security Hub CSPM console

Untuk memisahkan akun anggota yang diundang secara manual

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensi akun administrator.
2. Di panel navigasi, di bawah Pengaturan, pilih Konfigurasi.
3. Di bagian Akun, pilih akun yang ingin Anda pisahkan.

4. Pilih Tindakan, lalu pilih Disassociate account.

Security Hub CSPM API

Untuk memisahkan akun anggota yang diundang secara manual

Memanggil `DisassociateMembers`API dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda pisahkan. Untuk melihat daftar akun anggota, gunakan `ListMembers`operasi.

AWS CLI

Untuk memisahkan akun anggota yang diundang secara manual

Jalankan `disassociate-members`perintah dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda pisahkan. Untuk melihat daftar akun anggota, jalankan `list-members`perintah.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Contoh

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Menghapus akun anggota di Security Hub CSPM

> **Note**
>
> Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations.

Sebagai akun administrator CSPM AWS Security Hub, Anda dapat menghapus akun anggota yang ditambahkan melalui undangan. Sebelum Anda dapat menghapus akun yang diaktifkan, Anda harus memisahkannya.

Ketika Anda menghapus akun anggota, itu sepenuhnya dihapus dari daftar. Untuk memulihkan keanggotaan akun, Anda harus menambahkan dan mengundangnya lagi seolah-olah itu adalah akun anggota yang sama sekali baru.

Anda tidak dapat menghapus akun milik organisasi dan yang dikelola menggunakan integrasi denganAWS Organizations.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus akun anggota yang diundang secara manual.

Security Hub CSPM console

Untuk menghapus akun anggota yang diundang secara manual

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan akun administrator.
2. Di panel navigasi, pilih Pengaturan, lalu pilih Konfigurasi.
3. Pilih tab Akun undangan. Kemudian, pilih akun yang akan dihapus.
4. Pilih Tindakan, lalu pilih Hapus. Opsi ini hanya tersedia jika Anda telah memisahkan akun. Anda harus memisahkan akun anggota sebelum dapat dihapus.

Security Hub CSPM API

Untuk menghapus akun anggota yang diundang secara manual

Memanggil `DeleteMembers`API dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda hapus. Untuk mengambil daftar akun anggota, panggil API. `ListMembers`

AWS CLI

Untuk menghapus akun anggota yang diundang secara manual

Jalankan `delete-members`perintah dari akun administrator. Anda harus memberikan Akun AWS ID akun anggota yang ingin Anda hapus. Untuk mengambil daftar akun anggota, jalankan `list-members`perintah.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Contoh

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Memutuskan hubungan dari akun administrator CSPM Security Hub

> **Note**
>
> Sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations.

Jika akun Anda ditambahkan sebagai akun anggota CSPM AWS Security Hub melalui undangan, Anda dapat memisahkan akun anggota dari akun administrator. Setelah Anda memisahkan akun anggota, Security Hub CSPM tidak mengirimkan temuan dari akun ke akun administrator.

Akun anggota yang dikelola menggunakan integrasi dengan tidak AWS Organizations dapat memisahkan akun mereka dari akun administrator. Hanya administrator yang didelegasikan CSPM Security Hub yang dapat memisahkan akun anggota yang dikelola dengan Organizations.

Ketika Anda memisahkan diri dari akun administrator Anda, akun Anda tetap berada dalam daftar anggota akun administrator dengan status Mengundurkan diri. Namun, akun administrator tidak menerima temuan apa pun untuk akun Anda.

Setelah Anda memisahkan diri dari akun administrator, undangan untuk menjadi anggota masih tetap ada. Anda dapat menerima undangan lagi di masa depan.

Security Hub CSPM console

Untuk memisahkan diri dari akun administrator

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Pengaturan, lalu pilih Akun.
3. Di bagian Akun Administrator, matikan Terima, lalu pilih Perbarui.

Security Hub CSPM API

Untuk memisahkan diri dari akun administrator Anda

Memanggil `DisassociateFromAdministratorAccount`API.

AWS CLI

Untuk memisahkan diri dari akun administrator Anda

Jalankan perintah `disassociate-from-administrator-account`.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Konsol CSPM Security Hub terus digunakan. `DisassociateFromMasterAccount` Ini pada akhirnya akan berubah untuk digunakan`DisassociateFromAdministratorAccount`. Setiap kebijakan IAM yang secara khusus mengontrol akses ke fungsi ini harus terus digunakan`DisassociateFromMasterAccount`. Anda juga harus menambahkan kebijakan Anda `DisassociateFromAdministratorAccount` untuk memastikan bahwa izin yang benar diberlakukan setelah konsol mulai digunakan`DisassociateFromAdministratorAccount`.

Transisi ke Organizations untuk mengelola akun di Security Hub CSPM

Ketika Anda mengelola akun secara manual di AWS Security Hub CSPM, Anda harus mengundang akun calon anggota dan mengonfigurasi setiap akun anggota secara terpisah di masing-masing akun. Wilayah AWS

Dengan mengintegrasikan Security Hub CSPM danAWS Organizations, Anda dapat menghilangkan kebutuhan untuk mengirim undangan dan mendapatkan kontrol lebih besar atas bagaimana Security Hub CSPM dikonfigurasi dan disesuaikan di organisasi Anda. Untuk alasan ini, sebaiknya gunakan AWS Organizations bukan undangan CSPM Security Hub untuk mengelola akun anggota Anda. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations.

Anda dapat menggunakan pendekatan gabungan di mana Anda menggunakan AWS Organizations integrasi, tetapi juga mengundang akun secara manual di luar organisasi Anda. Namun, kami merekomendasikan secara eksklusif menggunakan integrasi Organizations. Konfigurasi pusat, fitur yang membantu Anda mengelola CSPM Security Hub di beberapa akun dan Wilayah, hanya tersedia saat Anda berintegrasi dengan Organizations.

Bagian ini mencakup bagaimana Anda dapat beralih dari manajemen akun berbasis undangan manual ke mengelola akun dengan. AWS Organizations

Mengintegrasikan CSPM Security Hub denganAWS Organizations

Pertama, Anda harus mengintegrasikan Security Hub CSPM dan. AWS Organizations

Anda dapat mengintegrasikan layanan ini dengan menyelesaikan langkah-langkah berikut:

- Buat organisasi diAWS Organizations. Untuk petunjuk, lihat Membuat organisasi di Panduan AWS Organizations Pengguna.
- Dari akun manajemen Organizations, tentukan akun administrator yang didelegasikan CSPM Security Hub.

> **Note**
>
> Akun manajemen organisasi tidak dapat ditetapkan sebagai akun DA.

Untuk petunjuk mendetail, lihat Mengintegrasikan CSPM Security Hub denganAWS Organizations.

Dengan menyelesaikan langkah-langkah sebelumnya, Anda memberikan akses tepercaya untuk Security Hub CSPM di. AWS Organizations Ini juga memungkinkan Security Hub CSPM saat ini Wilayah AWS untuk akun administrator yang didelegasikan.

Administrator yang didelegasikan dapat mengelola organisasi di Security Hub CSPM, terutama dengan menambahkan akun organisasi sebagai akun anggota CSPM Security Hub. Administrator juga dapat mengakses pengaturan, data, dan sumber daya CSPM Security Hub tertentu untuk akun tersebut.

Saat Anda beralih ke manajemen akun menggunakan Organizations, akun berbasis undangan tidak secara otomatis menjadi anggota CSPM Security Hub. Hanya akun yang Anda tambahkan ke organisasi baru yang dapat menjadi anggota CSPM Security Hub.

Setelah mengaktifkan integrasi, Anda dapat mengelola akun dengan Organizations. Untuk informasi, lihat Mengelola Security Hub CSPM untuk beberapa akunAWS Organizations. Manajemen akun bervariasi berdasarkan jenis konfigurasi organisasi Anda.

Tindakan yang diizinkan oleh administrator dan akun anggota di Security Hub CSPM

Akun administrator dan anggota memiliki akses ke tindakan CSPM AWS Security Hub yang dicatat dalam tabel berikut. Dalam tabel, nilai-nilai memiliki arti sebagai berikut:

- Apa saja — Akun dapat melakukan tindakan untuk akun anggota mana pun di bawah administrator yang sama.
- Saat ini — Akun dapat melakukan tindakan hanya untuk dirinya sendiri (akun yang saat ini Anda masuki).
- Dash — Menunjukkan bahwa akun tidak dapat melakukan tindakan.

Sebagaimana dicatat dalam tabel, tindakan yang diizinkan berbeda berdasarkan apakah Anda berintegrasi dengan AWS Organizations dan jenis konfigurasi yang digunakan organisasi Anda. Untuk informasi tentang perbedaan antara konfigurasi pusat dan lokal, lihatMengelola akun denganAWS Organizations.

Security Hub CSPM tidak menyalin temuan akun anggota ke akun administrator. Di Security Hub CSPM, semua temuan dicerna ke Wilayah tertentu untuk akun tertentu. Di setiap Wilayah, akun administrator dapat melihat dan mengelola temuan untuk akun anggota mereka di Wilayah tersebut.

Jika Anda menetapkan Wilayah agregasi, akun administrator dapat melihat dan mengelola temuan akun anggota dari Wilayah tertaut yang direplikasi ke Wilayah agregasi. Untuk informasi selengkapnya tentang agregasi lintas wilayah, lihat Cross-Region agregasi.

Tabel berikut menentukan izin default untuk akun administrator dan anggota. Anda dapat menggunakan kebijakan IAM khusus untuk membatasi akses lebih lanjut ke fitur dan fungsi CSPM Security Hub. Untuk panduan dan contoh, lihat posting blog Menyelaraskan kebijakan IAM ke persona pengguna untuk AWS Security Hub CSPM.

Tindakan yang diizinkan jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi pusat

Akun administrator dan anggota dapat mengakses tindakan CSPM Security Hub sebagai berikut jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi pusat.

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota yang dikelola secara terpusat	Self-managed akun anggota
Membuat dan mengelola kebijakan konfigurasi CSPM Security Hub	Untuk akun yang dikelola sendiri dan terpusat	–	–
Lihat akun organisasi	Setiap	–	–
Putuskan akun anggota	Setiap	–	–
Hapus akun anggota	Akun non-organisasi apa pun	–	–
Nonaktifkan CSPM Security Hub	Untuk akun saat ini dan akun yang dikelola secara terpusat	–	Saat ini (harus dipisahkan dari akun administrator)
Lihat temuan dan temukan sejarah	Setiap	Saat ini	Saat ini
Perbarui temuan	Setiap	Saat ini	Saat ini
Lihat hasil wawasan	Setiap	Saat ini	Saat ini
Lihat detail kontrol	Setiap	Saat ini	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol konsolidasi	Setiap	–	–
Mengaktifkan dan menonaktifkan standar	Untuk akun saat ini dan akun yang	–	Saat ini

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota yang dikelola secara terpusat	Self-managed akun anggota
	dikelola secara terpusat		
Aktifkan dan nonaktifkan kontrol	Untuk akun saat ini dan akun yang dikelola secara terpusat	–	Saat ini
Mengaktifkan dan menonaktifkan integrasi	Saat ini	Saat ini	Saat ini
Konfigurasikan agregasi lintas wilayah	Setiap	–	–
Pilih beranda Wilayah dan terkait Wilayah	Apa saja (harus berhenti dan memulai ulang konfigurasi pusat untuk mengubah Wilayah rumah)	–	–
Konfigurasikan tindakan khusus	Saat ini	Saat ini	Saat ini
Konfigurasikan aturan otomatisasi	Setiap	–	–
Konfigurasikan wawasan khusus	Saat ini	Saat ini	Saat ini

Tindakan yang diizinkan jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi lokal

Akun administrator dan anggota dapat mengakses tindakan CSPM Security Hub sebagai berikut jika Anda berintegrasi dengan Organizations dan menggunakan konfigurasi lokal.

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota
Membuat dan mengelola kebijakan konfigurasi CSPM Security Hub	–	–
Lihat akun organisasi	Setiap	–
Putuskan akun anggota	Setiap	–
Hapus akun anggota	–	–
Nonaktifkan CSPM Security Hub	–	Saat ini (jika akun dipisahkan dari administrator yang didelegasikan)
Lihat temuan dan temukan sejarah	Setiap	Saat ini
Perbarui temuan	Setiap	Saat ini
Lihat hasil wawasan	Setiap	Saat ini
Lihat detail kontrol	Setiap	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol konsolidasi	Setiap	–
Mengaktifkan dan menonaktifkan standar	Saat ini	Saat ini

Tindakan	Security Hub CSPM mendelegasikan akun administrator	Akun anggota
Secara otomatis mengaktif kan CSPM Security Hub dan standar default di akun organisasi baru	Untuk akun saat ini dan akun organisasi baru	–
Aktifkan dan nonaktifkan kontrol	Saat ini	Saat ini
Mengaktifkan dan menonakti fkan integrasi	Saat ini	Saat ini
Konfigurasikan agregasi lintas wilayah	Setiap	–
Konfigurasikan tindakan khusus	Saat ini	Saat ini
Konfigurasikan aturan otomatisasi	Setiap	–
Konfigurasikan wawasan khusus	Saat ini	Saat ini

Tindakan yang diizinkan untuk akun berbasis undangan

Akun administrator dan anggota dapat mengakses tindakan CSPM Security Hub sebagai berikut jika Anda menggunakan metode berbasis undangan untuk mengelola akun secara manual, bukan mengintegrasikan dengan. AWS Organizations

Tindakan	Akun administrator CSPM Security Hub	Akun anggota
Membuat dan mengelola kebijakan konfigurasi CSPM Security Hub	–	–
Lihat akun organisasi	Setiap	–
Putuskan akun anggota	Setiap	Saat ini
Hapus akun anggota	Setiap	–
Nonaktifkan CSPM Security Hub	Saat ini (jika tidak ada akun anggota yang diaktifkan)	Saat ini (jika akun dipisahkan dari akun administrator)
Lihat temuan dan temukan sejarah	Setiap	Saat ini
Perbarui temuan	Setiap	Saat ini
Lihat hasil wawasan	Setiap	Saat ini
Lihat detail kontrol	Setiap	Saat ini
Mengaktifkan atau menonaktifkan temuan kontrol konsolidasi	Setiap	–
Mengaktifkan dan menonaktifkan standar	Saat ini	Saat ini
Secara otomatis mengaktifkan CSPM Security Hub dan standar default di akun organisasi baru	–	–
Aktifkan dan nonaktifkan kontrol	Saat ini	Saat ini

Tindakan	Akun administrator CSPM Security Hub	Akun anggota
Mengaktifkan dan menonakti fkan integrasi	Saat ini	Saat ini
Konfigurasikan agregasi lintas wilayah	Setiap	–
Konfigurasikan tindakan khusus	Saat ini	Saat ini
Konfigurasikan aturan otomatisasi	Setiap	–
Konfigurasikan wawasan khusus	Saat ini	Saat ini

Pengaruh tindakan akun pada data CSPM Security Hub

Tindakan akun ini memiliki efek berikut pada data CSPM AWS Security Hub.

Security Hub CSPM dinonaktifkan

Jika Anda menggunakan konfigurasi pusat, administrator yang didelegasikan (DA) dapat membuat kebijakan konfigurasi CSPM Security Hub yang menonaktifkan CSPM AWS Security Hub di akun tertentu dan unit organisasi (OU). Dalam hal ini, CSPM Security Hub dinonaktifkan di akun dan OU yang ditentukan di Wilayah asal Anda dan Wilayah yang ditautkan. Jika Anda tidak menggunakan konfigurasi pusat, Anda harus menonaktifkan Security Hub CSPM secara terpisah di setiap akun dan Wilayah tempat Anda mengaktifkannya. Anda tidak dapat menggunakan konfigurasi pusat jika Security Hub CSPM dinonaktifkan di akun DA.

Tidak ada temuan yang dihasilkan atau diperbarui untuk akun administrator jika CSPM Security Hub dinonaktifkan di akun administrator. Temuan arsip yang ada dihapus setelah 30 hari. Temuan aktif yang ada dihapus setelah 90 hari.

Integrasi dengan Layanan AWS yang lain dihapus.

Standar dan kontrol keamanan yang diaktifkan dinonaktifkan.

Data dan pengaturan CSPM Security Hub lainnya, termasuk tindakan kustom, wawasan, dan langganan produk pihak ketiga disimpan selama 90 hari.

Akun anggota dipisahkan dari akun administrator

Ketika akun anggota dipisahkan dari akun administrator, akun administrator kehilangan izin untuk melihat temuan di akun anggota. Namun, Security Hub CSPM masih diaktifkan di kedua akun.

Jika Anda menggunakan konfigurasi pusat, DA tidak dapat mengonfigurasi CSPM Security Hub untuk akun anggota yang dipisahkan dari akun DA.

Pengaturan atau integrasi khusus yang ditentukan untuk akun administrator tidak diterapkan pada temuan dari akun anggota sebelumnya. Misalnya, setelah akun dipisahkan, Anda mungkin memiliki tindakan kustom di akun administrator yang digunakan sebagai pola peristiwa dalam EventBridge aturan Amazon. Namun, tindakan kustom ini tidak dapat digunakan di akun anggota.

Dalam daftar Akun untuk akun administrator CSPM Security Hub, akun yang dihapus memiliki status Terputus.

Akun anggota dihapus dari organisasi

Ketika akun anggota dihapus dari organisasi, akun administrator CSPM Security Hub kehilangan izin untuk melihat temuan di akun anggota. Namun, Security Hub CSPM masih diaktifkan di kedua akun dengan pengaturan yang sama sebelum dihapus.

Jika Anda menggunakan konfigurasi pusat, Anda tidak dapat mengonfigurasi CSPM Security Hub untuk akun anggota setelah dihapus dari organisasi tempat administrator yang didelegasikan berada. Namun, akun mempertahankan pengaturan yang dimilikinya sebelum dihapus kecuali Anda mengubahnya secara manual.

Dalam daftar Akun untuk akun administrator CSPM Security Hub, akun yang dihapus memiliki status Dihapus.

Akun ditangguhkan

Ketika Akun AWS ditangguhkan, akun kehilangan izin untuk melihat temuan mereka di Security Hub CSPM. Tidak ada temuan yang dihasilkan atau diperbarui untuk akun itu. Akun administrator untuk akun yang ditangguhkan dapat melihat temuan yang ada untuk akun tersebut.

Untuk akun organisasi, status akun anggota juga dapat berubah menjadi Akun Ditangguhkan. Ini terjadi jika akun ditangguhkan pada saat yang sama ketika akun administrator mencoba mengaktifkan akun. Akun administrator untuk akun yang Ditangguhkan Akun tidak dapat melihat

temuan untuk akun tersebut. Jika tidak, status yang ditangguhkan tidak akan memengaruhi status akun anggota.

Jika Anda menggunakan konfigurasi pusat, asosiasi kebijakan gagal jika administrator yang didelegasikan mencoba mengaitkan kebijakan konfigurasi dengan akun yang ditangguhkan.

Setelah 90 hari, akun dihentikan atau diaktifkan kembali. Ketika akun diaktifkan kembali, izin CSPM Security Hub akan dipulihkan. Jika status akun anggota adalah Akun Ditangguhkan, akun administrator harus mengaktifkan akun secara manual.

Akun ditutup

Ketika Akun AWS ditutup, Security Hub CSPM merespons penutupan sebagai berikut.

Jika akun tersebut adalah akun administrator CSPM Security Hub, akun tersebut dihapus sebagai akun administrator dan semua akun anggota dihapus. Jika akun tersebut adalah akun anggota, akun tersebut dipisahkan dan dihapus sebagai anggota dari akun administrator CSPM Security Hub.

Security Hub CSPM menyimpan temuan arsip yang ada di akun selama 30 hari. Untuk temuan kontrol, perhitungan 30 hari didasarkan pada nilai untuk `UpdatedAt` bidang temuan. Untuk jenis temuan lain, perhitungan didasarkan pada nilai untuk `UpdatedAt` atau `ProcessedAt` bidang temuan, tanggal mana pun yang terbaru. Pada akhir periode 30 hari ini, Security Hub CSPM secara permanen menghapus temuan dari akun.

Security Hub CSPM mempertahankan temuan aktif yang ada di akun selama 90 hari. Untuk temuan kontrol, perhitungan 90 hari didasarkan pada nilai untuk `UpdatedAt` bidang temuan. Untuk jenis temuan lain, perhitungan didasarkan pada nilai untuk `UpdatedAt` atau `ProcessedAt` bidang temuan, tanggal mana pun yang terbaru. Pada akhir periode 90 hari ini, Security Hub CSPM secara permanen menghapus temuan dari akun.

Untuk retensi jangka panjang dari temuan yang ada, Anda dapat mengekspor temuan ke ember S3. Anda dapat melakukan ini dengan menggunakan tindakan kustom dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat Menggunakan EventBridge untuk respon otomatis dan remediasi.

> **Important**
>
> Untuk pelanggan yang masukAWS GovCloud (US) Regions, buat cadangan, lalu hapus data kebijakan dan sumber daya akun lainnya sebelum menutup akun. Anda tidak akan memiliki akses ke sumber daya dan data setelah menutup akun.

Untuk informasi selengkapnya, lihat Menutup Akun AWS di Panduan AWS Account Management Referensi.

Memahami agregasi lintas wilayah di Security Hub CSPM

> **Note**
>
> Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Dengan menggunakan agregasi Lintas wilayah di CSPM AWS Security Hub, Anda dapat mengumpulkan temuan, menemukan pembaruan, wawasan, mengontrol status kepatuhan, dan skor keamanan dari beberapa ke satu Wilayah asal. Wilayah AWS Anda kemudian dapat mengelola semua data ini dari Wilayah asal.

Misalkan Anda menetapkan US East (Virginia N.) sebagai Wilayah asal, dan AS Barat (Oregon) dan AS Barat (California N.) sebagai Wilayah terkait. Ketika Anda melihat halaman Temuan di AS Timur (Virginia N.), Anda melihat temuan dari ketiga Wilayah. Pembaruan temuan tersebut juga tercermin di ketiga Wilayah.

> **Note**
>
> DiAWS GovCloud (US), agregasi lintas wilayah hanya didukung untuk temuan, menemukan pembaruan, dan wawasan di seluruh wilayah. AWS GovCloud (US) Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara AWS GovCloud (US-East) dan AWS GovCloud (US-West). Di Wilayah Tiongkok, agregasi lintas wilayah hanya didukung untuk temuan, menemukan pembaruan, dan wawasan di seluruh Wilayah Tiongkok. Secara khusus, Anda hanya dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan antara Tiongkok (Beijing) dan Tiongkok (Ningxia).

Jika kontrol diaktifkan di Wilayah tertaut tetapi dinonaktifkan di Wilayah asal, Anda dapat melihat status kepatuhan kontrol dari Wilayah asal, tetapi Anda tidak dapat mengaktifkan atau menonaktifkan kontrol tersebut dari Wilayah asal. Pengecualiannya adalah jika Anda menggunakan konfigurasi pusat. Jika Anda menggunakan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat mengonfigurasi kontrol di Wilayah beranda dan Wilayah tertaut dari Wilayah beranda.

Jika Anda telah menetapkan Wilayah asal, skor keamanan memperhitungkan status kontrol di semua Wilayah terkait. Untuk melihat skor keamanan lintas wilayah dan status kepatuhan, tambahkan izin berikut ke peran IAM Anda yang menggunakan CSPM Security Hub:

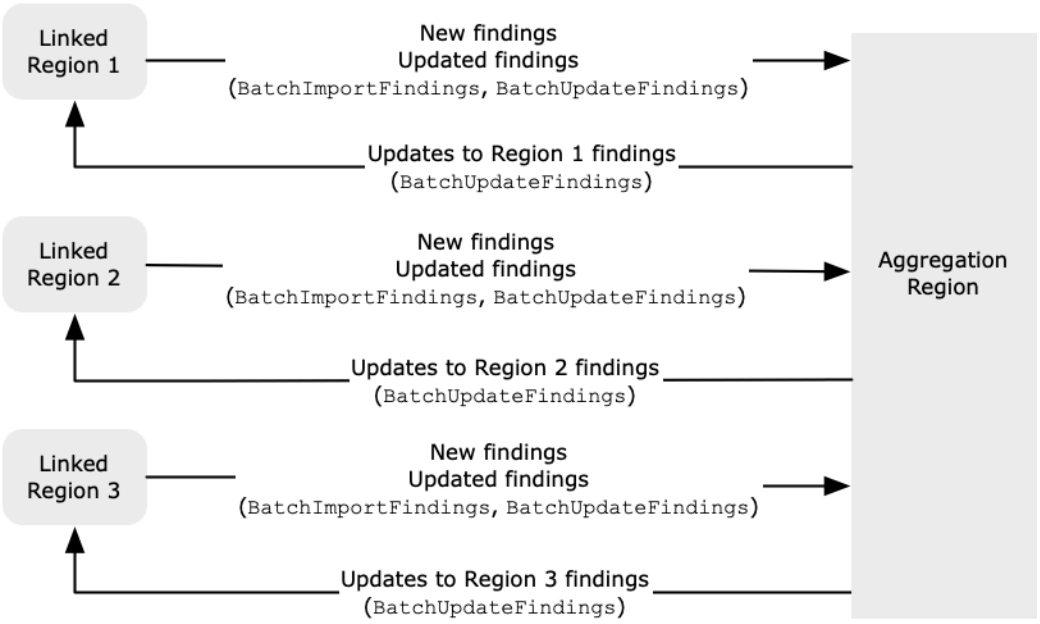
- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`
- `BatchUpdateStandardsControlAssociations`

Jenis data yang dikumpulkan

Bila agregasi lintas wilayah diaktifkan dengan satu atau beberapa Wilayah tertaut, Security Hub CSPM mereplikasi data berikut dari Wilayah tertaut ke Wilayah asal. Ini terjadi di setiap akun yang mengaktifkan agregasi lintas wilayah.

- Temuan
- Wawasan
- Mengontrol status kepatuhan
- Skor keamanan

Selain data baru dalam daftar sebelumnya, Security Hub CSPM juga mereplikasi pembaruan data ini antara Wilayah tertaut dan Wilayah asal. Pembaruan yang terjadi di Wilayah tertaut direplikasi ke Wilayah asal. Pembaruan yang terjadi di Wilayah asal direplikasi kembali ke Wilayah yang ditautkan. Jika ada pembaruan yang bertentangan di Wilayah asal dan Wilayah yang ditautkan, maka pembaruan terbaru digunakan.



Cross-Region agregasi tidak menambah biaya Security Hub CSPM. Anda tidak dikenakan biaya saat Security Hub CSPM mereplikasi data atau pembaruan baru.

Di Wilayah beranda, halaman Ringkasan memberikan tampilan temuan aktif Anda di seluruh Wilayah yang ditautkan. Untuk informasi, lihat Melihat ringkasan temuan lintas wilayah berdasarkan tingkat keparahan. Panel halaman Ringkasan lainnya yang menganalisis temuan juga menampilkan informasi dari seluruh Wilayah yang ditautkan.

Skor keamanan Anda di Wilayah asal dihitung dengan membandingkan jumlah kontrol yang diteruskan dengan jumlah kontrol yang diaktifkan di semua Wilayah yang ditautkan. Selain itu, jika kontrol diaktifkan di setidaknya satu Wilayah yang ditautkan, kontrol akan terlihat di halaman detail standar Keamanan di Wilayah asal. Status kepatuhan kontrol pada halaman detail standar mencerminkan temuan di seluruh Wilayah terkait. Jika pemeriksaan keamanan yang terkait dengan kontrol gagal di satu atau beberapa Wilayah yang ditautkan, status kepatuhan kontrol tersebut akan ditampilkan sebagai Gagal pada halaman detail standar Wilayah beranda. Jumlah pemeriksaan keamanan mencakup temuan dari semua Wilayah terkait.

Security Hub CSPM hanya mengumpulkan data dari Wilayah di mana akun memiliki CSPM Security Hub diaktifkan. Security Hub CSPM tidak diaktifkan secara otomatis untuk akun berdasarkan konfigurasi agregasi lintas wilayah.

Agregasi lintas wilayah dapat diaktifkan tanpa Wilayah yang ditautkan dipilih. Dalam hal ini, tidak ada replikasi data yang terjadi.

Agregasi untuk akun administrator dan anggota

Akun mandiri, akun anggota, dan akun administrator dapat mengonfigurasi agregasi lintas wilayah. Jika dikonfigurasi oleh administrator, keberadaan akun administrator sangat penting agar agregasi lintas wilayah berfungsi di akun yang dikelola. Jika akun administrator dihapus atau dipisahkan dari akun anggota, agregasi lintas wilayah untuk akun anggota akan berhenti. Hal ini berlaku bahkan jika akun telah mengaktifkan agregasi lintas wilayah sebelum hubungan administrator-anggota dimulai.

Saat akun administrator mengaktifkan agregasi Lintas wilayah, CSPM Security Hub mereplikasi data yang dihasilkan akun administrator di semua Wilayah tertaut ke Wilayah beranda. Selain itu, Security Hub CSPM mengidentifikasi akun anggota yang terkait dengan administrator tersebut, dan setiap akun anggota mewarisi pengaturan agregasi lintas wilayah administrator. Security Hub CSPM mereplikasi data yang dihasilkan akun anggota di semua Wilayah tertaut ke Wilayah asal.

Administrator dapat mengakses dan mengelola temuan keamanan dari semua akun anggota dalam wilayah yang dikelola. Namun, sebagai administrator CSPM Security Hub, Anda harus masuk ke Wilayah beranda untuk melihat data gabungan dari semua akun anggota dan Wilayah yang ditautkan.

Sebagai akun anggota CSPM Security Hub, Anda harus masuk ke Wilayah beranda untuk melihat data agregat dari akun Anda dari semua Wilayah yang ditautkan. Akun anggota tidak memiliki izin untuk melihat data dari akun anggota lainnya.

Akun administrator dapat mengundang akun anggota secara manual atau berfungsi sebagai administrator yang didelegasikan dari organisasi yang terintegrasi dengannyaAWS Organizations. Untuk akun anggota yang diundang secara manual, administrator harus mengundang akun dari Wilayah asal dan semua Wilayah yang ditautkan agar agregasi Lintas wilayah berfungsi. Selain itu, akun anggota harus mengaktifkan CSPM Security Hub di Wilayah asal dan semua Wilayah yang ditautkan untuk memberikan administrator kemampuan untuk melihat temuan dari akun anggota. Jika Anda tidak menggunakan Wilayah asal untuk tujuan lain, Anda dapat menonaktifkan standar dan integrasi CSPM Security Hub di Wilayah tersebut untuk mencegah biaya.

Jika Anda berencana untuk menggunakan agregasi lintas wilayah, dan memiliki beberapa akun administrator, sebaiknya ikuti praktik terbaik berikut ini:

- Setiap akun administrator memiliki akun anggota yang berbeda.
- Setiap akun administrator memiliki akun anggota yang sama di seluruh Wilayah.
- Setiap akun administrator menggunakan Wilayah rumah yang berbeda.

> **Note**
>
> Untuk memahami bagaimana agregasi lintas wilayah memengaruhi konfigurasi pusat, lihat. Dampak konfigurasi pusat pada agregasi lintas wilayah

Dampak konfigurasi pusat pada agregasi lintas wilayah

Konfigurasi pusat adalah fitur opt-in di AWS Security Hub CSPM yang dapat Anda gunakan jika Anda berintegrasi dengannya. AWS Organizations Jika Anda menggunakan konfigurasi pusat, akun administrator yang didelegasikan dapat mengonfigurasi layanan, standar, dan kontrol CSPM Security Hub untuk akun dan unit organisasi (OU) dalam organisasi. Untuk mengonfigurasi akun dan OU, administrator yang didelegasikan membuat kebijakan konfigurasi CSPM Security Hub. Kebijakan konfigurasi dapat digunakan untuk menentukan apakah CSPM Security Hub diaktifkan atau dinonaktifkan, dan standar dan kontrol mana yang diaktifkan. Administrator yang didelegasikan mengaitkan kebijakan konfigurasi dengan akun tertentu, OU, atau root (seluruh organisasi).

Administrator yang didelegasikan dapat membuat dan mengelola kebijakan konfigurasi untuk organisasi hanya dari Wilayah asal. Selain itu, kebijakan konfigurasi berlaku di Wilayah asal dan semua Wilayah yang ditautkan. Anda tidak dapat membuat kebijakan konfigurasi yang hanya berlaku di beberapa Wilayah tertaut dan bukan yang lain. Untuk informasi tentang agregasi lintas wilayah, lihat Cross-Region agregasi.

Untuk menggunakan konfigurasi pusat, Anda harus menunjuk Wilayah rumah. Secara opsional, Anda dapat memilih satu atau beberapa Wilayah sebagai Wilayah yang ditautkan. Anda juga dapat memilih untuk menunjuk Wilayah asal tanpa Wilayah terkait.

Mengubah setelan agregasi lintas wilayah dapat memengaruhi kebijakan konfigurasi Anda. Saat Anda menambahkan Wilayah tertaut, kebijakan konfigurasi Anda akan berlaku di Wilayah tersebut. Jika Region adalah Region keikutsertaan, Region harus diaktifkan agar kebijakan konfigurasi Anda berlaku di sana. Sebaliknya, saat Anda menghapus Wilayah tertaut, kebijakan konfigurasi tidak lagi berlaku di Wilayah tersebut. Di Wilayah itu, akun mempertahankan pengaturan yang mereka miliki saat Wilayah yang ditautkan dihapus. Anda dapat mengubah pengaturan tersebut, tetapi harus melakukannya secara terpisah di setiap akun dan Wilayah.

Jika Anda menghapus atau mengubah Wilayah beranda, kebijakan konfigurasi dan asosiasi kebijakan Anda akan dihapus. Anda tidak dapat lagi menggunakan konfigurasi pusat atau membuat kebijakan konfigurasi di Wilayah mana pun. Akun mempertahankan pengaturan yang mereka miliki sebelum Wilayah asal diubah atau dihapus. Anda dapat mengubah pengaturan tersebut kapan saja,

tetapi karena Anda tidak lagi menggunakan konfigurasi pusat, pengaturan harus dimodifikasi secara terpisah di setiap akun dan Wilayah. Anda dapat menggunakan konfigurasi pusat dan membuat kebijakan konfigurasi lagi jika Anda menunjuk Wilayah rumah baru.

Untuk informasi selengkapnya tentang konfigurasi pusat, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Mengaktifkan agregasi lintas wilayah

> **Note**
>
> Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Anda harus mengaktifkan agregasi lintas wilayah dari Wilayah AWS yang ingin Anda tetapkan sebagai Wilayah asal.

Untuk mengaktifkan agregasi lintas wilayah, Anda membuat sumber daya CSPM Security Hub yang disebut agregator pencarian. Sumber daya agregator temuan menentukan Wilayah asal Anda dan Wilayah yang ditautkan (jika ada).

Anda tidak dapat menggunakan Wilayah AWS yang dinonaktifkan secara default sebagai Wilayah rumah Anda. Untuk daftar Wilayah yang dinonaktifkan secara default, lihat Mengaktifkan Wilayah di. Referensi Umum AWS

Bila Anda mengaktifkan agregasi lintas wilayah, Anda memilih untuk menentukan satu atau beberapa Wilayah tertaut jika diinginkan. Anda juga dapat memilih apakah akan secara otomatis menautkan Wilayah baru saat Security Hub CSPM mulai mendukungnya dan Anda telah memilihnya.

Security Hub CSPM console

Untuk mengaktifkan agregasi lintas wilayah

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Menggunakan Wilayah AWS pemilih, masuk ke Wilayah yang ingin Anda gunakan sebagai Wilayah agregasi.
3. Di menu navigasi CSPM Security Hub, pilih Settings dan kemudian Regions.
4. Untuk Menemukan agregasi, pilih Konfigurasikan agregasi pencarian.

Secara default, Region home diatur ke No agregasi Region.

5. Di bawah Wilayah Agregasi, pilih opsi untuk menetapkan Wilayah saat ini sebagai Wilayah asal.
6. Secara opsional, untuk Wilayah Tertaut, pilih Wilayah untuk mengumpulkan data.
7. Untuk secara otomatis menggabungkan data dari Wilayah baru di partisi sebagai Security Hub CSPM mendukungnya dan Anda memilihnya, pilih Tautkan Wilayah masa depan.
8. Pilih Simpan.

Security Hub CSPM API

Dari Region yang ingin Anda gunakan sebagai Wilayah asal, gunakan `CreateFindingAggregator`pengoperasian Security Hub CSPM API. Jika Anda menggunakanAWS CLI, jalankan perintah create-finding-aggregator.

Untuk`RegionLinkingMode`, pilih salah satu opsi berikut:

- `ALL_REGIONS`— Security Hub CSPM mengumpulkan data dari semua Wilayah. Security Hub CSPM juga mengumpulkan data dari Wilayah baru karena didukung dan Anda memilihnya.
- `ALL_REGIONS_EXCEPT_SPECIFIED`— Security Hub CSPM mengumpulkan data dari semua Wilayah kecuali untuk Wilayah yang ingin Anda kecualikan. Security Hub CSPM juga mengumpulkan data dari Wilayah baru karena didukung dan Anda memilihnya. Gunakan `Regions` untuk menyediakan daftar Wilayah untuk dikecualikan dari agregasi.
- `SPECIFIED_REGIONS`— Security Hub CSPM mengumpulkan data dari daftar Wilayah yang dipilih. Security Hub CSPM tidak mengumpulkan data secara otomatis dari Wilayah baru. Gunakan `Regions` untuk menyediakan daftar Wilayah untuk dikumpulkan dari.
- `NO_REGIONS`— Security Hub CSPM tidak mengumpulkan data karena Anda tidak memilih Wilayah yang ditautkan.

Contoh berikut mengkonfigurasi agregasi lintas wilayah. Wilayah asalnya adalah US East (Virginia N.). Wilayah yang terhubung adalah US West (California N.) dan US West (Oregon). Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Meninjau pengaturan agregasi lintas wilayah

> **Note**
>
> Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Anda dapat melihat konfigurasi agregasi Lintas wilayah saat ini di CSPM AWS Security Hub dari mana pun. Wilayah AWS Konfigurasi mencakup Wilayah asal, Wilayah yang ditautkan (jika ada), dan apakah akan secara otomatis menautkan Wilayah baru sebagai Security Hub CSPM mendukungnya.

Akun anggota dapat melihat setelan agregasi lintas wilayah yang dikonfigurasi oleh akun administrator.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat pengaturan agregasi lintas wilayah Anda saat ini.

Security Hub CSPM console

Untuk melihat setelan agregasi lintas wilayah (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, pilih Pengaturan dan kemudian tab Wilayah.

Jika agregasi lintas wilayah tidak diaktifkan, maka tab Wilayah menampilkan opsi untuk mengaktifkan agregasi lintas wilayah. Hanya akun administrator dan akun mandiri yang dapat mengaktifkan agregasi lintas wilayah.

Jika agregasi lintas wilayah diaktifkan, maka tab Wilayah menampilkan informasi berikut:

- Wilayah asal
- Apakah akan secara otomatis menggabungkan temuan, wawasan, status kontrol, dan skor keamanan dari Wilayah baru yang didukung CSPM Security Hub dan yang Anda pilih
- Daftar Wilayah tertaut (jika ada yang dipilih)

Security Hub CSPM API

Untuk meninjau setelan agregasi lintas wilayah (Security Hub CSPM API)

Gunakan `GetFindingAggregator`pengoperasian Security Hub CSPM API. Jika Anda menggunakanAWS CLI, jalankan perintah get-finding-aggregator.

Saat Anda membuat permintaan, berikan ARN agregator temuan. Untuk mendapatkan ARN agregator temuan, gunakan perintah operasi atau `ListFindingAggregators`list-finding-aggregator.

Contoh berikut menunjukkan pengaturan agregasi lintas wilayah untuk ARN agregator temuan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

Memperbarui pengaturan agregasi lintas wilayah

> **Note**
>
> Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Anda dapat memperbarui setelan agregasi Lintas wilayah saat ini di CSPM AWS Security Hub dengan mengubah Wilayah tertaut atau Wilayah beranda saat ini. Anda juga dapat mengubah apakah akan secara otomatis mengumpulkan data dari Wilayah AWS yang baru yang didukung CSPM Security Hub.

Perubahan pada agregasi Lintas wilayah tidak diterapkan untuk Wilayah keikutsertaan hingga Anda mengaktifkan Wilayah di wilayah Anda. Akun AWS Wilayah yang AWS diperkenalkan pada atau setelah hingga 20 Maret 2019 adalah Wilayah yang ikut serta.

Bila Anda berhenti menggabungkan data dari Wilayah tertaut, AWS Security Hub CSPM tidak menghapus data agregat yang ada dari Wilayah tersebut yang dapat diakses di Wilayah asal.

Anda tidak dapat menggunakan prosedur pembaruan di bagian ini untuk mengubah Wilayah beranda. Untuk mengubah wilayah rumah, Anda harus melakukan hal berikut:

1. Hentikan agregasi lintas wilayah. Untuk petunjuk, lihat the section called “Menghentikan agregasi”.

2. Ubah ke Wilayah yang Anda inginkan menjadi Wilayah asal baru.
3. Aktifkan agregasi lintas wilayah. Untuk petunjuk, lihat the section called “Mengaktifkan agregasi”.

Anda harus memperbarui konfigurasi agregasi lintas wilayah dari Wilayah rumah saat ini.

Security Hub CSPM console

Untuk mengubah Wilayah yang ditautkan

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk ke Wilayah agregasi saat ini.
2. Di menu navigasi CSPM Security Hub, pilih Pengaturan, lalu pilih Wilayah.
3. Untuk Menemukan agregasi, pilih Edit.
4. Untuk Wilayah Tertaut, perbarui Wilayah tertaut yang dipilih.
5. Jika perlu, ubah apakah Link future Regions dipilih. Pengaturan ini menentukan apakah Security Hub CSPM secara otomatis menautkan Wilayah baru karena menambahkan dukungan untuk mereka dan Anda memilihnya.
6. Pilih Simpan.

Security Hub CSPM API

Gunakan `UpdateFindingAggregator`operasi. Jika Anda menggunakanAWS CLI, jalankan perintah update-finding-aggregator. Untuk mengidentifikasi agregator temuan, Anda harus memberikan agregator temuan ARN. Untuk mendapatkan ARN agregator temuan, gunakan perintah operasi atau `ListFindingAggregators`list-finding-aggregator..

Jika mode penautan adalah `ALL_REGIONS_EXCEPT_SPECIFIED` atau`SPECIFIED_REGIONS`, Anda dapat mengubah daftar Wilayah yang dikecualikan atau disertakan. Jika Anda ingin mengubah mode penautan Wilayah ke`NO_REGIONS`, Anda tidak boleh memberikan daftar Wilayah.

Ketika Anda mengubah daftar Wilayah yang dikecualikan atau disertakan, Anda harus memberikan daftar lengkap dengan pembaruan. Misalnya, Anda saat ini mengumpulkan temuan dari US East (Ohio), dan ingin juga mengumpulkan temuan dari US West (Oregon). Anda harus memberikan `Regions` daftar yang berisi US East (Ohio) dan US West (Oregon).

Contoh berikut memperbarui agregasi lintas wilayah ke Wilayah yang dipilih. Perintah dijalankan dari Wilayah asal saat ini, yaitu US East (Virginia N.). Wilayah yang terhubung adalah US West (California N.) dan US West (Oregon). Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-
aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-
aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode
 SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Menghentikan agregasi lintas wilayah

> **Note**
>
> Wilayah agregasi sekarang disebut Wilayah asal. Beberapa operasi Security Hub CSPM API masih menggunakan istilah agregasi Region yang lebih lama.

Jika Anda tidak ingin AWS Security Hub CSPM mengumpulkan data, Anda dapat menghapus agregator temuan Anda. Atau, Anda dapat menyimpan agregator temuan Anda tetapi tidak menautkan apa pun Wilayah AWS ke Wilayah rumah dengan memperbarui agregator yang ada ke mode `NO_REGIONS` penautan.

Untuk mengubah Wilayah rumah Anda, Anda harus menghapus agregator temuan Anda saat ini dan membuat yang baru.

Ketika Anda menghapus agregator temuan Anda, Security Hub CSPM berhenti menggabungkan data. Itu tidak menghapus data agregat yang ada dari Wilayah asal.

Menghapus agregator temuan (konsol)

Anda dapat menghapus agregator temuan Anda dari Wilayah beranda saat ini saja.

Di Wilayah selain Wilayah rumah, panel agregasi Menemukan di konsol CSPM Security Hub menampilkan pesan bahwa Anda harus mengedit konfigurasi di Wilayah beranda. Pilih pesan ini untuk menampilkan tautan untuk beralih ke Wilayah beranda.

Security Hub CSPM console

Untuk menghentikan agregasi lintas wilayah (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pastikan Anda masuk ke Wilayah asal Anda saat ini.
3. Di menu navigasi CSPM Security Hub, pilih Pengaturan, lalu pilih Wilayah.
4. Di bawah Menemukan agregasi, pilih Edit.
5. Di bawah Wilayah Agregasi, pilih Tidak ada Wilayah agregasi.
6. Pilih Simpan.
7. Pada dialog konfirmasi, di bidang konfirmasi, ketik**`Confirm`**.
8. Pilih Konfirmasi.

Security Hub CSPM API

Gunakan `DeleteFindingAggregator`pengoperasian Security Hub CSPM API. Jika Anda menggunakanAWS CLI, jalankan `delete-finding-aggregator`perintah.

Untuk mengidentifikasi agregator temuan yang akan dihapus, berikan ARN agregator temuan. Untuk mendapatkan ARN agregator temuan, gunakan operasi `list-finding-aggregators`atau `ListFindingAggregators`perintah.

Contoh berikut menghapus agregator temuan. Perintah dijalankan dari Wilayah asal saat ini, yaitu US East (Virginia N.). Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-
east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --
region us-east-1
```

Memahami standar keamanan di Security Hub CSPM

Di AWS Security Hub CSPM, standar keamanan adalah seperangkat persyaratan yang didasarkan pada kerangka peraturan, praktik terbaik industri, atau kebijakan perusahaan. Untuk detail tentang standar yang didukung Security Hub CSPM saat ini, termasuk kontrol keamanan yang berlaku untuk masing-masing standar, lihat. Referensi standar untuk Security Hub CSPM

Saat Anda mengaktifkan standar, Security Hub CSPM secara otomatis mengaktifkan semua kontrol yang berlaku untuk standar. Security Hub CSPM kemudian menjalankan pemeriksaan keamanan pada kontrol, yang menghasilkan temuan Security Hub CSPM. Anda dapat menonaktifkan dan kemudian mengaktifkan kembali kontrol individual seperlunya. Anda juga dapat menonaktifkan standar sepenuhnya. Jika Anda menonaktifkan standar, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan pada kontrol yang berlaku untuk standar. Temuan tidak lagi dihasilkan untuk kontrol.

Selain temuan, Security Hub CSPM menghasilkan skor keamanan untuk setiap standar yang Anda aktifkan. Skor didasarkan pada status kontrol yang berlaku untuk standar. Jika Anda menetapkan Wilayah agregasi, skor keamanan untuk standar mencerminkan status kontrol di semua Wilayah yang ditautkan. Jika Anda adalah administrator CSPM Security Hub untuk suatu organisasi, skor tersebut mencerminkan status kontrol untuk semua akun di organisasi Anda. Untuk informasi selengkapnya, lihat Menghitung skor keamanan.

Untuk meninjau dan mengelola standar, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Di konsol, halaman Standar keamanan menampilkan semua standar keamanan yang didukung Security Hub CSPM saat ini. Ini termasuk deskripsi setiap standar dan status standar saat ini. Jika Anda mengaktifkan standar, Anda juga dapat menggunakan halaman ini untuk mengakses detail tambahan untuk standar. Misalnya, Anda dapat meninjau:

- Skor keamanan saat ini untuk standar.
- Statistik agregat untuk kontrol yang berlaku untuk standar.
- Daftar kontrol yang berlaku untuk standar dan saat ini diaktifkan, termasuk status kepatuhan masing-masing.
- Daftar kontrol yang berlaku untuk standar tetapi saat ini dinonaktifkan.

Untuk analisis yang lebih mendalam, Anda dapat memfilter dan mengurutkan data, dan menelusuri ke bawah untuk meninjau detail kontrol individual yang berlaku untuk standar.

Anda dapat mengaktifkan standar secara individual untuk satu akun dan Wilayah AWS. Namun, untuk menghemat waktu dan mengurangi penyimpangan konfigurasi di lingkungan multi-akun dan Multi-wilayah, sebaiknya gunakan konfigurasi pusat untuk mengaktifkan dan mengelola standar. Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan yang menentukan cara mengonfigurasi standar di beberapa akun dan Wilayah.

Topik

- Referensi standar untuk Security Hub CSPM
- Mengaktifkan standar keamanan
- Meninjau detail standar keamanan
- Mematikan standar keamanan yang diaktifkan secara otomatis
- Menonaktifkan standar keamanan

Referensi standar untuk Security Hub CSPM

Di AWS Security Hub CSPM, standar keamanan adalah seperangkat persyaratan yang didasarkan pada kerangka peraturan, praktik terbaik industri, atau kebijakan perusahaan. Security Hub CSPM memetakan persyaratan ini ke kontrol, dan menjalankan pemeriksaan keamanan pada kontrol untuk menilai apakah persyaratan standar terpenuhi. Setiap standar mencakup beberapa kontrol.

Security Hub CSPM saat ini mendukung standar berikut:

- AWS Praktik Terbaik Keamanan Dasar — Dikembangkan oleh AWS dan profesional industri, standar ini adalah kompilasi praktik terbaik keamanan untuk organisasi, terlepas dari sektor atau ukurannya. Ini menyediakan serangkaian kontrol yang mendeteksi kapan Anda Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan. Ini juga memberikan panduan preskriptif tentang cara meningkatkan dan mempertahankan postur keamanan Anda.
- Praktik Terbaik Keamanan AI — Dikembangkan oleh pakar AWS keamanan, standar ini menyediakan serangkaian kontrol yang dikuratori yang mendeteksi kapan sumber daya AI yang digunakan tidak selaras dengan praktik terbaik keamanan. Ini membantu Anda mengidentifikasi area di mana beban kerja AI Anda menyimpang dari konfigurasi keamanan yang disarankan, mencakup domain seperti isolasi jaringan, enkripsi, penempatan VPC, dan AWS KMS penggunaan kunci.
- AWS Penandaan Sumber Daya — Dikembangkan oleh Security Hub CSPM, standar ini dapat membantu Anda menentukan apakah AWS sumber daya Anda memiliki tag. Tag adalah pasangan kunci-nilai yang bertindak sebagai metadata untuk sumber daya. AWS Tag dapat membantu Anda mengidentifikasi, mengkategorikan, mengelola, dan mencari AWS sumber daya. Misalnya, Anda dapat menggunakan tag untuk mengkategorikan sumber daya berdasarkan tujuan, pemilik, atau lingkungan.
- CIS AWS Foundations Benchmark — Dikembangkan oleh Center for Internet Security (CIS), standar ini menyediakan pedoman konfigurasi yang aman untuk AWS. Ini menentukan seperangkat pedoman konfigurasi keamanan dan praktik terbaik untuk subset Layanan AWS dan sumber daya, dengan penekanan pada pengaturan dasar, dapat diuji, dan arsitektur agnostik.

Pedoman tersebut mencakup prosedur implementasi dan penilaian langkah demi langkah yang jelas.

- NIST SP 800-53 Revisi 5 — Standar ini sejalan dengan persyaratan National Institute of Standards and Technology (NIST) untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya penting. Kerangka kerja terkait umumnya berlaku untuk U.S. lembaga federal atau organisasi yang bekerja dengan U.S. lembaga federal atau sistem informasi. Namun, organisasi swasta juga dapat menggunakan persyaratan sebagai kerangka panduan.
- NIST SP 800-171 Revisi 2 - Standar ini sejalan dengan rekomendasi dan persyaratan keamanan NIST untuk melindungi kerahasiaan Informasi Tidak Terklasifikasi Terkendali (CUI) dalam sistem dan organisasi yang bukan bagian dari. pemerintah federal. U.S CUI adalah informasi yang tidak memenuhi kriteria pemerintah untuk klasifikasi, tetapi dianggap sensitif dan dibuat atau dimiliki ole U.S h. pemerintah federal atau entitas lain atas nama U.S. pemerintah federal.
- PCI DSS — Standar ini sejalan dengan kerangka kepatuhan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) yang ditentukan oleh Dewan Standar Keamanan PCI (SSC). Kerangka kerja ini menyediakan seperangkat aturan dan pedoman untuk menangani informasi kartu kredit dan debit dengan aman. Kerangka kerja umumnya berlaku untuk organisasi yang menyimpan, memproses, atau mengirimkan data pemegang kartu.
- Service-managed standar, AWS Control Tower — Standar ini membantu Anda mengonfigurasi kontrol detektif yang disediakan oleh Security Hub CSPM dari. AWS Control Tower AWS Control Tower menawarkan cara mudah untuk mengatur dan mengatur lingkungan AWS multi-akun, mengikuti praktik terbaik preskriptif.

Standar dan kontrol CSPM Hub Keamanan tidak menjamin kepatuhan terhadap kerangka peraturan atau audit apa pun. Sebaliknya, mereka menyediakan cara untuk mengevaluasi dan memantau keadaan Anda Akun AWS dan sumber daya. Sebaiknya aktifkan setiap standar yang relevan dengan kebutuhan bisnis, industri, atau kasus penggunaan Anda.

Kontrol individu dapat diterapkan ke lebih dari satu standar. Jika Anda mengaktifkan beberapa standar, sebaiknya Anda juga mengaktifkan temuan kontrol konsolidasi. Jika Anda melakukan ini, Security Hub CSPM menghasilkan satu temuan untuk setiap kontrol, bahkan jika kontrol tersebut berlaku untuk lebih dari satu standar. Jika Anda tidak mengaktifkan temuan kontrol konsolidasi, Security Hub CSPM menghasilkan temuan terpisah untuk setiap standar yang diaktifkan yang diterapkan kontrol. Misalnya, jika Anda mengaktifkan dua standar dan kontrol berlaku untuk keduanya, Anda menerima dua temuan terpisah untuk kontrol, satu untuk setiap standar. Jika Anda mengaktifkan temuan kontrol konsolidasi, Anda hanya menerima satu temuan untuk kontrol. Untuk informasi selengkapnya, lihat Temuan kontrol konsolidasi.

Referensi terperinci dengan standar

- AWS Standar Praktik Terbaik Keamanan Dasar di Security Hub CSPM
- Standar Praktik Terbaik Keamanan AI di Security Hub CSPM
- AWS Standar Penandaan Sumber Daya di Security Hub CSPM
- CIS AWS Benchmark Yayasan di Hub Keamanan CSPM
- NIST SP 800-53 Revisi 5 di Hub Keamanan CSPM
- NIST SP 800-171 Revisi 2 di Hub Keamanan CSPM
- PCI DSS di Hub Keamanan CSPM
- Service-managed standar dalam Security Hub CSPM

AWS Standar Praktik Terbaik Keamanan Dasar di Security Hub CSPM

Dikem AWS bangkan oleh para profesional industri, standar F AWS oundational Security Best Practices (FSBP) adalah kompilasi praktik terbaik keamanan untuk organisasi, terlepas dari sektor atau ukuran organisasi. Ini menyediakan serangkaian kontrol yang mendeteksi kapan Akun AWS dan sumber daya menyimpang dari praktik terbaik keamanan. Ini juga memberikan panduan preskriptif tentang cara meningkatkan dan mempertahankan postur keamanan organisasi Anda.

Di AWS Security Hub CSPM, standar Praktik AWS Terbaik Keamanan Dasar mencakup kontrol yang terus mengevaluasi beban kerja Anda Akun AWS dan beban kerja, serta membantu Anda mengidentifikasi area yang menyimpang dari praktik terbaik keamanan. Kontrol mencakup praktik terbaik keamanan untuk sumber daya dari banyak sumber daya Layanan AWS. Setiap kontrol diberi kategori yang mencerminkan fungsi keamanan yang diterapkan kontrol. Untuk daftar kategori dan detail tambahan, lihatKategori kontrol.

Kontrol yang berlaku untuk standar

Daftar berikut menentukan kontrol CSPM AWS Security Hub mana yang berlaku untuk standar Praktik Terbaik AWS Keamanan Dasar (v1.0.0). Untuk meninjau detail kontrol, pilih kontrol.

[Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS

[ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu

[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

[APIGateway.1] API Gateway REST dan logging eksekusi WebSocket API harus diaktifkan

[APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

[APIGateway.3] Tahap API REST API Gateway harus memiliki AWS X-Ray pelacakan diaktifkan

[APIGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF

[APIGateway.5] Data cache API REST API Gateway harus dienkripsi saat diam

[APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi

[APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages

[APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi

[APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan

[AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat

[AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan

[AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API

[AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit

[Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

[AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone

[AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)

[Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

[AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone

[AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2

[Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat

[BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC

[BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk

[BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik

[BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi

[CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi

[CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait

[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

[CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit

[CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi

Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging

[CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

[CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus

[CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

[CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus

[CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

[CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada

[CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

[CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan

Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal

Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas

[CodeBuild.3] CodeBuild Log S3 harus dienkripsi

[CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil

[CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat

[Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi

[Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat

[Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus

[Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito

[Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan

[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat

[DataSync.1] DataSync tugas harus mengaktifkan logging

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

[DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging

[DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging

[DMS.9] Titik akhir DMS harus menggunakan SSL

[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM

[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

[DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS

[DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone

[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

[DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan

[DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit

[DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas dengan permintaan

[DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time

[DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan

[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit

[EC2.1] Snapshot Amazon EBS tidak boleh dikonfigurasi agar dapat dipulihkan secara publik

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.3] Volume Amazon EBS yang terlampir harus dienkripsi saat istirahat

[EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

[EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik

[EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2

[EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik

[EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

[EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI

[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

[EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi

[EC2.20] Kedua terowongan VPN untuk AWS Site-to-Site Koneksi VPN harus aktif

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389

[EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC

[EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan

[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan

[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

[EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API

[EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry

[EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager

[EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager

[EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager

[EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)

[EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging

[EC2.172] Pengaturan Akses Publik Blok VPC EC2 harus memblokir lalu lintas gateway internet

[EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir

[EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination

[EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir

[EC2.182] Blokir pengaturan akses publik harus diaktifkan untuk snapshot Amazon EBS

[EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2

[ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

[ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi

[ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi

[ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis

[ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host

[ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa

[ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root

[ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging

[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru

[ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer

[ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik

[ECS.18] Definisi Tugas ECS harus menggunakan enkripsi dalam transit untuk volume EFS

[ECS.19] Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi yang dikelola

[ECS.20] Definisi Tugas ECS harus mengkonfigurasi pengguna non-root dalam definisi wadah Linux

[ECS.21] Definisi Tugas ECS harus mengkonfigurasi pengguna non-administrator dalam definisi wadah Windows

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

[EFS.2] Volume Amazon EFS harus dalam rencana cadangan

[EFS.3] Titik akses EFS harus menerapkan direktori root

[EFS.4] Titik akses EFS harus menegakkan identitas pengguna

[EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis

[EFS.8] Sistem file EFS harus dienkripsi saat diam

[EKS.1] Titik akhir cluster EKS tidak boleh diakses publik

[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung

[EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi

[EKS.8] Cluster EKS harus mengaktifkan logging audit

[EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung

[ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis

[ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis

[ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis

[ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat

[ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan

[ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH

[ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default

[ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

[ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

[ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS

[ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager

[ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS

[ELB.4] Application Load Balancer harus dikonfigurasi untuk menghapus header http yang tidak valid

[ELB.5] Aplikasi dan pencatatan Penyeimbang Beban Klasik harus diaktifkan

[ELB.6] Aplikasi, Gateway, dan Penyeimbang Beban Jaringan harus mengaktifkan perlindungan penghapusan

[ELB.7] Classic Load Balancer harus mengaktifkan pengeringan koneksi

[ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki kekuatan AWS Config urasi

[ELB.9] Penyeimbang Beban Klasik harus mengaktifkan penyeimbangan beban lintas zona

[ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan

[ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan

[ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan

[ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit

[ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi

[ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi

[EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik

[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan

[EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat

[EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

[ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik

[ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

[ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan

[ES.5] Domain Elasticsearch harus mengaktifkan logging audit

[ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data

[ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus

[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

[FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

[FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan

[FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ

[FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ

[FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ

[Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat

[Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue

[GuardDuty.1] GuardDuty harus diaktifkan

[GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan

[GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan

[GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan

[GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan

[GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan

[GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan

[GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan

[GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus

[IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan

[Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan

[Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan

[Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan

[Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan

[Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat

[Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai

[KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS

[KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS

[KMS.3]AWS KMS keystidak boleh dihapus secara tidak sengaja

[KMS.5] Kunci KMS tidak boleh diakses publik

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung

[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan

[Macie.1] Amazon Macie harus diaktifkan

[Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

[MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch

[MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker

[MSK.3] Konektor MSK Connect harus dienkripsi saat transit

[MSK.4] Kluster MSK harus menonaktifkan akses publik

[MSK.5] Konektor MSK seharusnya mengaktifkan logging

[MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi

[Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat

[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch

[Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik

[Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

[Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis

[Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat

[Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM

[Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot

[NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

[NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait

[NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh

[NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

[NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

[NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan

[NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

[Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik

[Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

[Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan

[Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

[Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data

[Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

[Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru

[PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan

[Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS

[RDS.1] Snapshot RDS harus bersifat pribadi

[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat diam

[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Zona Ketersediaan

[RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans DB RDS

[RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan

[RDS.8] Instans DB RDS harus mengaktifkan perlindungan penghapusan

[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch

[RDS.10] Otentikasi IAM harus dikonfigurasi untuk instans RDS

[RDS.11] Instans RDS harus mengaktifkan cadangan otomatis

[RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS

[RDS.13] Upgrade versi minor otomatis RDS harus diaktifkan

[RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking

[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan

[RDS.16] Cluster Aurora DB harus dikonfigurasi untuk menyalin tag ke snapshot DB

[RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

[RDS.19] Langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa cluster kritis

[RDS.20] Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting

[RDS.21] Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting

[RDS.22] Langganan notifikasi peristiwa RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting

[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database

[RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus

[RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

[RDS.27] Cluster RDS DB harus dienkripsi saat diam

[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log

[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

[RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch

[RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch

[RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch

[RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit

[RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch

[RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi

[RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit

[RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit

[RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet

[RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB

[RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB

[RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan

[RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

[Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit

[Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis

[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit

[Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama

[Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan

[Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default

[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat

[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi

[Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ

[RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan

[RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL

[RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik

[RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default

[RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS

[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.9] Bucket tujuan umum S3 harus mengaktifkan logging akses server

[S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3

[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup

[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok

[S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok

[S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup

[SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung

[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

[SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook

[SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1

[SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan

[SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung

[SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer

[SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

[SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan

[SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan

[SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

[SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan

[SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

[SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama

[SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys

[SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer

[SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis

[SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar

[SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan

[SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu

[ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja

[SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email

[SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik

[SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat

[SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik

[SSM.1] Instans Amazon EC2 harus dikelola olehAWS Systems Manager

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

[SSM.4] Dokumen SSM seharusnya tidak bersifat publik

[SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan

[SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik

[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging

[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

[Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging

[WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan

[WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat

[WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan

[WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan

[WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat

[WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan

[WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

[WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan

[WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik

[WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat

[WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Standar Praktik Terbaik Keamanan AI di Security Hub CSPM

Standar Praktik Terbaik Keamanan AI adalah serangkaian pemeriksaan keamanan otomatis yang mendeteksi kapan sumber daya AI yang digunakan tidak selaras dengan praktik terbaik keamanan. Dikembangkan oleh pakar AWS keamanan, standar ini menyediakan serangkaian kontrol yang dikuratori yang membantu Anda mengidentifikasi area di mana beban kerja AI Anda menyimpang dari konfigurasi keamanan yang direkomendasikan.

Di AWS Security Hub CSPM, standar Praktik Terbaik Keamanan AI mencakup kontrol yang terus mengevaluasi sumber daya Anda. Kontrol mencakup domain keamanan termasuk tetapi tidak terbatas pada isolasi jaringan, enkripsi saat istirahat dan dalam transit, penempatan VPC, penggunaan AWS KMS kunci, dan persyaratan registri pribadi. Setiap kontrol diberi kategori yang mencerminkan fungsi keamanan yang diterapkan kontrol. Untuk daftar kategori dan detail tambahan, lihatKategori kontrol di Security Hub CSPM.

Standar Praktik Terbaik Keamanan AI memiliki Nama Sumber Daya Amazon (ARN) berikut:`arn:aws:securityhub:`*`region`*`::standards/ai-security-best-practices/v/1.0.0`, di *`region`* mana kode Wilayah untuk yang berlaku Wilayah AWS. Anda juga dapat menggunakan GetEnabledStandards operasi Security Hub CSPM API untuk mengambil ARN dari standar yang saat ini diaktifkan.

Kontrol yang berlaku untuk standar

Daftar berikut menentukan kontrol CSPM AWS Security Hub mana yang berlaku untuk standar Praktik Terbaik Keamanan AI (v1.0.0). Untuk meninjau detail kontrol, pilih kontrol.

- [Bedrock.1] Sumber data Amazon Bedrock harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk

- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [BedrockAgentCore.7] Interpreter kode AgentCore kustom batuan dasar harus menggunakan konfigurasi jaringan pribadi
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys

- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SageMaker.20] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.21] instance SageMaker notebook harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [SageMaker.22] jadwal SageMaker pemantauan harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.23] eksperimen SageMaker inferensi harus memiliki volume penyimpanan instance yang dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [SageMaker.24] eksperimen SageMaker inferensi harus memiliki penyimpanan data yang dienkripsi dengan pengelolaan pelanggan AWS KMS keys
- [SageMaker.25] definisi pekerjaan kualitas SageMaker model harus mengaktifkan isolasi jaringan

AWS Standar Penandaan Sumber Daya di Security Hub CSPM

Standar AWS Resource Tagging, yang dikembangkan oleh AWS Security Hub CSPM, membantu Anda menentukan apakah AWS sumber daya Anda memiliki tag yang hilang. Tag adalah pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur AWS sumber daya. Dengan sebagian besar AWS sumber daya, Anda memiliki opsi untuk menambahkan tag ke sumber daya saat Anda membuat sumber daya atau setelah Anda membuat sumber daya. Contoh sumber daya termasuk CloudFront distribusi Amazon, instans Amazon Elastic Compute Cloud (Amazon EC2), dan rahasia di. AWS Secrets Manager Tag dapat membantu Anda mengelola, mengidentifikasi, mengatur, mencari, dan memfilter AWS sumber daya.

Setiap tag memiliki dua bagian:

- Kunci tag—misalnya,, `CostCenter` `Environment`, atau. `Project` Kunci tag peka huruf besar dan kecil.
- Nilai tag—misalnya, `111122223333` atau. `Production` Seperti kunci tag, nilai tag peka huruf besar dan kecil.

Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk informasi tentang menambahkan tag ke AWS sumber daya, lihat Panduan Pengguna Sumber AWS Daya Tagging dan Editor Tag.

Untuk setiap kontrol yang berlaku untuk standar AWS Penandaan Sumber Daya di Security Hub CSPM, Anda dapat menggunakan parameter yang didukung secara opsional untuk menentukan kunci tag yang ingin kontrol periksa. Jika Anda tidak menentukan kunci tag apa pun, kontrol hanya memeriksa keberadaan setidaknya satu kunci tag, dan gagal jika sumber daya tidak memiliki kunci tag.

Sebelum Anda mengaktifkan standar Pen AWS andaan Sumber Daya, penting untuk mengaktifkan dan mengonfigurasi perekaman sumber daya di AWS Config. Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis AWS sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Jika tidak, Security Hub CSPM mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku untuk standar. Untuk informasi selengkapnya, termasuk daftar jenis sumber daya yang akan direkam, lihatAWS ConfigSumber daya yang diperlukan untuk temuan kontrol.

Setelah mengaktifkan standar Pen AWS andaan Sumber Daya, Anda mulai menerima temuan untuk kontrol yang berlaku untuk standar. Perhatikan bahwa diperlukan waktu hingga 18 jam bagi Security Hub CSPM untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS Config terkait layanan yang sama dengan kontrol yang berlaku untuk standar lain yang diaktifkan. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Standar AWS Penandaan Sumber Daya memiliki Nama Sumber Daya Amazon (ARN) berikut:`arn:aws:securityhub:`*`region`*`::standards/aws-resource-tagging-standard/v/1.0.0`, di *`region`* mana kode Wilayah untuk yang berlaku Wilayah AWS. Anda juga dapat menggunakan GetEnabledStandards operasi Security Hub CSPM API untuk mengambil ARN dari standar yang saat ini diaktifkan.

> **Note**
>
> Standar AWS Penandaan Sumber Daya tidak tersedia di Wilayah Asia Pasifik (Selandia Baru) dan Asia Pasifik (Taipei).

Kontrol yang berlaku untuk standar

Daftar berikut menentukan kontrol CSPM AWS Security Hub mana yang berlaku untuk standar AWS Resource Tagging (v1.0.0). Untuk meninjau detail kontrol, pilih kontrol.

- [ACM.3] Sertifikat ACM harus ditandai
- [Amplify.1] Amplify aplikasi harus ditandai

- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.4]AWS AppSyncGraphQL API harus diberi tag
- [Athena.2] Katalog data Athena harus ditandai
- [Athena.3] Kelompok kerja Athena harus ditandai
- [AutoScaling.10] Grup EC2 Auto Scaling harus diberi tag
- [Backup.2]AWS Backuppoin pemulihan harus ditandai
- [Backup.3]AWS Backupbrankas harus diberi tag
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Backup.5]AWS Backuprencana cadangan harus ditandai
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudTrail.9] CloudTrail jejak harus ditandai
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai

- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DynamoDB.5] Tabel DynamoDB harus diberi tag
- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.35] Antarmuka jaringan EC2 harus ditandai
- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.37] Alamat IP Elastis EC2 harus ditandai
- [EC2.38] Instans EC2 harus ditandai
- [EC2.39] Gerbang internet EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.41] ACL jaringan EC2 harus ditandai
- [EC2.42] Tabel rute EC2 harus ditandai
- [EC2.43] Grup keamanan EC2 harus ditandai
- [EC2.44] Subnet EC2 harus ditandai
- [EC2.45] Volume EC2 harus ditandai
- [EC2.46] Amazon VPC harus ditandai
- [EC2.47] Layanan titik akhir Amazon VPC harus diberi tag
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.49] Koneksi peering VPC Amazon harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.52] Gerbang transit EC2 harus ditandai
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [ECR.4] Repositori publik ECR harus diberi tag

- [ECS.13] Layanan ECS harus ditandai
- [ECS.14] Cluster ECS harus ditandai
- [ECS.15] Definisi tugas ECS harus ditandai
- [EFS.5] Titik akses EFS harus diberi tag
- [EKS.6] Cluster EKS harus diberi tag
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.2] bus EventBridge acara harus ditandai
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.1]AWS Gluepekerjaan harus diberi tag
- [GuardDuty.2] GuardDuty filter harus ditandai
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag

- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.2] Aliran Kinesis harus ditandai
- [Lambda.6] Fungsi lambda harus ditandai
- [MQ.4] Broker Amazon MQ harus ditandai
- [NetworkFirewall.7] Firewall Firewall Jaringan harus ditandai
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai
- [Opensearch.9] OpenSearch domain harus ditandai
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.28] Cluster DB RDS harus diberi tag
- [RDS.29] Snapshot cluster RDS DB harus diberi tag
- [RDS.30] Instans DB RDS harus diberi tag
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.32] Snapshot DB RDS harus diberi tag
- [RDS.33] Grup subnet RDS DB harus diberi tag
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.13] Snapshot klaster Redshift harus diberi tag
- [Redshift.14] Grup subnet cluster Redshift harus diberi tag
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag

- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SecretsManager.5] Rahasia Secrets Manager harus ditandai
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SNS.3] Topik SNS harus ditandai
- [SQS.2] Antrian SQS harus ditandai
- [SSM.5] Dokumen SSM harus ditandai
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1]AWS Transfer Familyalur kerja harus diberi tag
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag

CIS AWS Benchmark Yayasan di Hub Keamanan CSPM

Benchmark Foundation Center for Internet Security (CIS) AWS berfungsi sebagai sekumpulan praktik terbaik konfigurasi keamanan untuk AWS. Praktik terbaik yang diterima industri ini memberi Anda prosedur implementasi dan penilaian langkah demi langkah yang jelas. Mulai dari sistem operasi hingga layanan cloud dan perangkat jaringan, kontrol dalam tolok ukur ini membantu Anda melindungi sistem spesifik yang digunakan organisasi Anda.

AWS Security Hub CSPM mendukung CIS Foun AWS dations Benchmark versi 5.0.0, 3.0.0, 1.4.0, dan 1.2.0. Halaman ini mencantumkan kontrol keamanan yang didukung setiap versi. Ini juga memberikan perbandingan versi.

CIS AWS Foundations Benchmark versi 5.0.0

Security Hub CSPM mendukung versi 5.0.0 (v5.0.0) dari CIS Foundations Benchmark. AWS Security Hub CSPM telah memenuhi persyaratan Sertifikasi Perangkat Lunak Keamanan CIS dan telah dianugerahi Sertifikasi Perangkat Lunak Keamanan CIS untuk Benchmark CIS berikut:

- Tolok Ukur CIS untuk Bench AWS mark Yayasan CIS, v5.0.0, Level 1

- Tolok Ukur CIS untuk Bench AWS mark Yayasan CIS, v5.0.0, Level 2

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark versi 5.0.0

[Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389

[EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh

[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

[EFS.8] Sistem file EFS harus dienkripsi saat diam

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan

[IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

[IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus

[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess

[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan

[KMS.4]AWS KMSrotasi kunci harus diaktifkan

[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Zona Ketersediaan

[RDS.13] Upgrade versi minor otomatis RDS harus diaktifkan

[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek

[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek

CIS AWS Foundations Benchmark versi 3.0.0

Security Hub CSPM mendukung versi 3.0.0 (v3.0.0) dari CIS Foundations Benchmark. AWS Security Hub CSPM telah memenuhi persyaratan Sertifikasi Perangkat Lunak Keamanan CIS dan telah dianugerahi Sertifikasi Perangkat Lunak Keamanan CIS untuk Benchmark CIS berikut:

- Tolok Ukur CIS untuk Bench AWS mark Yayasan CIS, v3.0.0, Level 1
- Tolok Ukur CIS untuk Bench AWS mark Yayasan CIS, v3.0.0, Level 2

Kontrol yang berlaku untuk CIS AWS Foundations Benchmark versi 3.0.0

[Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389

[EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh

[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan

[IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

[IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus

[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess

[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan

[KMS.4]AWS KMSrotasi kunci harus diaktifkan

[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[RDS.13] Upgrade versi minor otomatis RDS harus diaktifkan

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek

[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek

CIS AWS Dasar Benchmark versi 1.4.0

Security Hub CSPM mendukung versi 1.4.0 (v1.4.0) dari CIS Foundations Benchmark. AWS

Kontrol yang berlaku untuk CIS AWS Dasar Benchmark versi 1.4.0

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi

[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi

[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi

[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan

[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)

[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan

[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute

[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.7] Enkripsi default EBS harus diaktifkan

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan

[IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

[KMS.4]AWS KMSrotasi kunci harus diaktifkan

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

CIS AWS Dasar Benchmark versi 1.2.0

Security Hub CSPM mendukung versi 1.2.0 (v1.2.0) dari CIS Foundations Benchmark. AWS Security Hub CSPM telah memenuhi persyaratan Sertifikasi Perangkat Lunak Keamanan CIS dan telah dianugerahi Sertifikasi Perangkat Lunak Keamanan CIS untuk Benchmark CIS berikut:

- Benchmark CIS untuk Bench AWS mark Yayasan CIS, v1.2.0, Level 1
- Benchmark CIS untuk Bench AWS mark Yayasan CIS, v1.2.0, Level 2

Kontrol yang berlaku untuk CIS AWS Dasar Benchmark versi 1.2.0

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah

[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA

[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi

[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi

[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi

[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan

[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)

[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan

[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute

[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22

[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol

[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor

[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang

[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan

[KMS.4]AWS KMSrotasi kunci harus diaktifkan

Perbandingan versi untuk CIS AWS Benchmark Yayasan

Bagian ini merangkum perbedaan antara versi tertentu dari Center for Internet Security (CIS) Foun AWS dations Benchmark — v5.0.0, v3.0.0, v1.4.0, dan v1.2.0. AWS Security Hub CSPM mendukung masing-masing versi CIS Foun AWS dations Benchmark ini. Namun, sebaiknya gunakan v5.0.0 agar tetap mengikuti praktik terbaik keamanan. Anda dapat mengaktifkan beberapa versi standar CIS Foun AWS dations Benchmark secara bersamaan. Untuk informasi tentang mengaktifkan standar, lihatMengaktifkan standar keamanan. Jika Anda ingin memutakhirkan ke v5.0.0, aktifkan sebelum Anda menonaktifkan versi yang lebih lama. Ini mencegah celah dalam pemeriksaan keamanan

Anda. Jika Anda menggunakan integrasi Security Hub CSPM dengan AWS Organizations dan ingin mengaktifkan batch v5.0.0 di beberapa akun, sebaiknya gunakan konfigurasi pusat. ???

Pemetaan kontrol ke persyaratan CIS di setiap versi

Memahami kontrol mana yang didukung setiap versi CIS Foun AWS dations Benchmark.

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS	1.2	1.2	1.2	1.18
[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	3.1	3.1	3.1	2.1
[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat	3.5	3.5	3.7	2.7
[CloudTrail.4] validasi file CloudTrail log harus diaktifkan	3.2	3.2	3.2	2.2
[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	3.4	2.4
[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	Tidak didukung — CIS menghapus	Tidak didukung — CIS menghapus	3.3	2.3

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
	persyaratan ini	persyaratan ini		
[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3	3.4	3.4	3.6	2.6
[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.3	3.3
[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	3.1
[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	3.2
[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.4	3.4
[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.5	3.5

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.6	3.6
[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.7	3.7
[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.8	3.8
[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.9	3.9
[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.10	3.10
[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.11	3.11

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.12	3.12
[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.13	3.13
[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	4.14	3.14
[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	3.3	3.3	3.5	2.5
[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	5.5	5.4	5.3	4.3
[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC	3.7	3.7	3.9	2.9
[EC2.7] Enkripsi default EBS harus diaktifkan	5.1.1	2.2.1	2.2.1	Tidak didukung

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)	5.7	5.6	Tidak didukung	Tidak didukung
[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22	Tidak didukung — diganti dengan persyaratan 5.3 dan 5.4	Tidak didukung - diganti dengan persyaratan 5.2 dan 5.3	Tidak didukung - diganti dengan persyaratan 5.2 dan 5.3	4.1
[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389	Tidak didukung — diganti dengan persyaratan 5.3 dan 5.4	Tidak didukung - diganti dengan persyaratan 5.2 dan 5.3	Tidak didukung - diganti dengan persyaratan 5.2 dan 5.3	4.2
[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389	5.2	5.1	5.1	Tidak didukung
[EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh	5.3	5.2	Tidak didukung	Tidak didukung
[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh	5.4	5.3	Tidak didukung	Tidak didukung

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS	2.3.1	2.4.1	Tidak didukung	Tidak didukung
[EFS.8] Sistem file EFS harus dienkripsi saat diam	2.3.1	Tidak didukung	Tidak didukung	Tidak didukung
[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh	Tidak didukung	Tidak didukung	1.16	1.22
[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan	1.14	1.15	Tidak didukung	1.16
[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang	1.13	1.14	1.14	1.4
[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada	1.3	1.4	1.4	1.12
[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	1.9	1.10	1.10	1.2
[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root	1.5	1.6	1.6	1.14

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus	Tidak didukung — lihat sebagai [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus gantinya	Tidak didukung — lihat sebagai [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus gantinya	Tidak didukung — lihat sebagai [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus gantinya	1.3
[IAM.9] MFA harus diaktifkan untuk pengguna root	1.4	1.5	1.5	1.13
[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	1.5
[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	1.6

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	1.7
[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	1.8
[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih	1.7	1.8	1.8	1.9
[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	1.8	1.9	1.9	1.10
[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	1.11
[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan	1.16	1.17	1.17	1.2

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.20] Hindari penggunaan pengguna root	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	Tidak didukung — CIS menghapus persyaratan ini	1.1
[IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus	1.11	1.12	1.12	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus	1.18	1.19	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess	1.21	1.22	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan	1.19	1.20	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[KMS.4]AWS KMSrotasi kunci harus diaktifkan	3.6	3.6	3.8	2.8
[Macie.1] Amazon Macie harus diaktifkan	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual	Tidak didukung - pemeriksaan manual
[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible	2.2.3	2.3.3	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat	2.2.1	2.3.1	2.3.1	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Zona Ketersediaan	2.2.4	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[RDS.13] Upgrade versi minor otomatis RDS harus diaktifkan	2.2.2	2.3.2	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan	2.2.4	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok	2.1.4	2.1.4	2.1.5	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS	2.1.1	2.1.1	2.1.2	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru
[S3.8] Bucket tujuan umum S3 harus memblokir akses publik	2.1.4	2.1.4	2.1.5	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

ID kontrol dan judul	Persyaratan CIS v5.0.0	Persyaratan CIS v3.0.0	Persyaratan CIS v1.4.0	Persyaratan CIS v1.2.0
[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	2.1.2	2.1.2	2.1.3	Tidak didukung - CIS menambahkan persyaratan ini di versi yang lebih baru

ARN untuk CIS AWS Tolok Ukur Yayasan

Ketika Anda mengaktifkan satu atau beberapa versi CIS Foun AWS dations Benchmark, Anda mulai menerima temuan dalam Format Pen AWS emuan Keamanan (ASFF). Di ASFF, setiap versi menggunakan Nama Sumber Daya Amazon (ARN) berikut:

Tolok U AWS kur Yayasan CIS v5.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/5.0.0
```

Tolok U AWS kur Yayasan CIS v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Benchmark AWS Yayasan CIS v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Benchmark AWS Yayasan CIS v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Anda dapat menggunakan pen GetEnabledStandards goperasian Security Hub CSPM API untuk menemukan ARN dari standar yang diaktifkan.

Nilai sebelumnya adalah untuk`StandardsArn`. Namun, `StandardsSubscriptionArn` mengacu pada sumber daya langganan standar yang dibuat CSPM Security Hub saat Anda berlangganan standar dengan menelepon BatchEnableStandards di Wilayah.

> **Note**
>
> Saat Anda mengaktifkan versi CIS Foun AWS dations Benchmark, diperlukan waktu hingga 18 jam bagi Security Hub CSPM untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS Config terkait layanan yang sama dengan kontrol yang diaktifkan di standar lain yang diaktifkan. Untuk informasi lebih lanjut tentang jadwal untuk menghasilkan temuan kontrol, lihatJadwal untuk menjalankan pemeriksaan keamanan.

Bidang pencarian berbeda jika Anda mengaktifkan temuan kontrol konsolidasi. Untuk informasi tentang perbedaan ini, lihatDampak konsolidasi pada bidang dan nilai ASFF. Untuk temuan kontrol sampel, lihatSampel temuan kontrol.

Persyaratan CIS yang tidak didukung di Security Hub CSPM

Seperti disebutkan dalam tabel sebelumnya, Security Hub CSPM tidak mendukung setiap persyaratan CIS di setiap versi CIS Foun AWS dations Benchmark. Banyak persyaratan yang tidak didukung hanya dapat dievaluasi dengan meninjau status AWS sumber daya Anda secara manual.

NIST SP 800-53 Revisi 5 di Hub Keamanan CSPM

Publikasi Khusus NIST 800-53 Revisi 5 (NIST SP 800-53 Rev. 5) adalah kerangka kerja keamanan siber dan kepatuhan yang dikembangkan oleh National Institute of Standards and Technology (NIST), sebuah lembaga yang merupakan bagian dari. U.S Departemen Perdagangan. Kerangka kepatuhan ini menyediakan katalog persyaratan keamanan dan privasi untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya penting. U.S. lembaga pemerintah federal dan kontraktor harus mematuhi persyaratan ini untuk melindungi sistem dan organisasi mereka. Organisasi swasta juga dapat secara sukarela menggunakan persyaratan sebagai kerangka panduan untuk mengurangi risiko keamanan siber. Untuk informasi lebih lanjut tentang kerangka kerja dan persyaratannya, lihat NIST SP 800-53 Rev. 5 di Pusat Sumber Daya Keamanan Kom puter NIST.

AWS Security Hub CSPM menyediakan kontrol keamanan yang mendukung subset persyaratan NIST SP 800-53 Revisi 5. Kontrol melakukan pemeriksaan keamanan otomatis untuk sumber Layanan AWS daya tertentu. Untuk mengaktifkan dan mengelola kontrol ini, Anda dapat mengaktifkan kerangka kerja NIST SP 800-53 Revisi 5 sebagai standar di Security Hub CSPM.

Perhatikan bahwa kontrol tidak mendukung persyaratan NIST SP 800-53 Revisi 5 yang memerlukan pemeriksaan manual.

Tidak seperti kerangka kerja lain, kerangka kerja NIST SP 800-53 Revisi 5 tidak preskriptif tentang bagaimana persyaratannya harus dievaluasi. Sebaliknya, kerangka kerja memberikan pedoman. Di Security Hub CSPM, standar dan kontrol NIST SP 800-53 Revisi 5 mewakili pemahaman layanan tentang pedoman ini.

Topik

- Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar
- Menentukan kontrol mana yang berlaku untuk standar

Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar

Untuk mengoptimalkan cakupan dan keakuratan temuan, penting untuk mengaktifkan dan mengkonfigurasi perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar NIST SP 800-53 Revisi 5 di AWS Security Hub CSPM. Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis AWS sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Ini terutama untuk kontrol yang memiliki jenis jadwal yang dipicu perubahan. Namun, beberapa kontrol dengan tipe jadwal periodik juga memerlukan perekaman sumber daya. Jika perekaman sumber daya tidak diaktifkan atau dikonfigurasi dengan benar, Security Hub CSPM mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku untuk standar.

Untuk informasi tentang cara Security Hub CSPM menggunakan perekaman sumber daya di AWS Config, lihat. Mengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM Untuk informasi tentang mengonfigurasi perekaman sumber daya di AWS Config, lihat Bek erja dengan perekam konfigurasi di Panduan AWS Config Pengembang.

Tabel berikut menentukan jenis sumber daya yang akan direkam untuk kontrol yang berlaku untuk standar NIST SP 800-53 Revisi 5 di Security Hub CSPM.

Layanan AWS	Jenis sumber daya
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`

Layanan AWS	Jenis sumber daya
AWS Backup	`AWS::Backup::RecoveryPoint`
Batu Dasar Amazon AgentCore	`AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Memory`
AWS Certificate Manager (ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service (AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Layanan AWS	Jenis sumber daya
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management (IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`

Layanan AWS	Jenis sumber daya
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`

Layanan AWS	Jenis sumber daya
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Menentukan kontrol mana yang berlaku untuk standar

Daftar berikut menentukan kontrol yang mendukung persyaratan NIST SP 800-53 Revisi 5 dan berlaku untuk standar NIST SP 800-53 Revisi 5 di AWS Security Hub CSPM. Untuk detail tentang persyaratan spesifik yang didukung kontrol, pilih kontrol. Kemudian lihat bidang Persyaratan terkait di detail untuk kontrol. Bidang ini menentukan setiap persyaratan NIST yang didukung kontrol. Jika bidang tidak menentukan persyaratan NIST tertentu, kontrol tidak mendukung persyaratan tersebut.

- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [APIGateway.1] API Gateway REST dan logging eksekusi WebSocket API harus diaktifkan
- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [APIGateway.3] Tahap API REST API Gateway harus memiliki AWS X-Ray pelacakan diaktifkan
- [APIGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [APIGateway.5] Data cache API REST API Gateway harus dienkripsi saat diam
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
- [CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
- [CloudTrail.4] validasi file CloudTrail log harus diaktifkan
- [CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys

- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [CloudWatch.16] CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas dengan permintaan
- [DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan

- [DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.1] Snapshot Amazon EBS tidak boleh dikonfigurasi agar dapat dipulihkan secara publik
- [EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
- [EC2.3] Volume Amazon EBS yang terlampir harus dienkripsi saat istirahat
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.7] Enkripsi default EBS harus diaktifkan
- [EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)
- [EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22
- [EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi
- [EC2.20] Kedua terowongan VPN untuk AWS Site-to-Site Koneksi VPN harus aktif
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EKS.1] Titik akhir cluster EKS tidak boleh diakses publik
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung

- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ELB.1] Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.4] Application Load Balancer harus dikonfigurasi untuk menghapus header http yang tidak valid
- [ELB.5] Aplikasi dan pencatatan Penyeimbang Beban Klasik harus diaktifkan
- [ELB.6] Aplikasi, Gateway, dan Penyeimbang Beban Jaringan harus mengaktifkan perlindungan penghapusan
- [ELB.7] Classic Load Balancer harus mengaktifkan pengeringan koneksi
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki kekuatan AWS Config urasi
- [ELB.9] Penyeimbang Beban Klasik harus mengaktifkan penyeimbangan beban lintas zona
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Penyeimbang Beban Aplikasi harus dikaitkan dengan AWS WAF ACL web
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [ES.5] Domain Elasticsearch harus mengaktifkan logging audit
- [ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data
- [ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus
- [ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.1] GuardDuty harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.3]AWS KMS keystidak boleh dihapus secara tidak sengaja
- [KMS.4]AWS KMSrotasi kunci harus diaktifkan
- [Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
- [Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung
- [Lambda.3] Fungsi lambda harus dalam VPC
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch

- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan

- [RDS.1] Snapshot RDS harus bersifat pribadi
- [RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible
- [RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat
- [RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat diam
- [RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Zona Ketersediaan
- [RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans DB RDS
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.8] Instans DB RDS harus mengaktifkan perlindungan penghapusan
- [RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch
- [RDS.10] Otentikasi IAM harus dikonfigurasi untuk instans RDS
- [RDS.11] Instans RDS harus mengaktifkan cadangan otomatis
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.13] Upgrade versi minor otomatis RDS harus diaktifkan
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan
- [RDS.16] Cluster Aurora DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.19] Langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa cluster kritis
- [RDS.20] Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting
- [RDS.21] Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting
- [RDS.22] Langganan notifikasi peristiwa RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting
- [RDS.23] Instans RDS tidak boleh menggunakan port default mesin database
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan

- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
- [S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik
- [S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik
- [S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS
- [S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS
- [S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
- [S3.8] Bucket tujuan umum S3 harus memblokir akses publik
- [S3.9] Bucket tujuan umum S3 harus mengaktifkan logging akses server
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan pembuatan versi

- [S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock
- [S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys
- [S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakanAWS KMS
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SSM.1] Instans Amazon EC2 harus dikelola olehAWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan

- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11]AWS WAFpencatatan ACL web harus diaktifkan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik

NIST SP 800-171 Revisi 2 di Hub Keamanan CSPM

Publikasi Khusus NIST 800-171 Revisi 2 (NIST SP 800-171 Rev. 2) adalah kerangka kerja keamanan siber dan kepatuhan yang dikembangkan oleh National Institute of Standards and Technology (NIST), sebuah lembaga yang merupakan bagian dari. U.S Departemen Perdagangan. Kerangka kepatuhan ini memberikan persyaratan keamanan yang direkomendasikan untuk melindungi kerahasiaan Informasi Tak Terklasifikasi Terkendali dalam sistem dan organisasi yang bukan bagian dari U.S. pemerintah federal. Informasi Tidak Terklasifikasi Terkendali, juga disebut sebagai CUI, adalah informasi sensitif yang tidak memenuhi kriteria pemerintah untuk klasifikasi tetapi harus dilindungi. Ini adalah informasi yang dianggap sensitif dan dibuat atau dimiliki ole U.S h. pemerintah federal atau entitas lain atas nama U.S. pemerintah federal.

NIST SP 800-171 Rev. 2 memberikan persyaratan keamanan yang direkomendasikan untuk melindungi kerahasiaan CUI ketika:

- Informasi tersebut berada dalam sistem dan organisasi non-federal,
- Organisasi non-federal tidak mengumpulkan atau memelihara informasi atas nama agen federal atau menggunakan atau mengoperasikan sistem atas nama agen, dan
- Tidak ada persyaratan pengamanan khusus untuk melindungi kerahasiaan CUI yang ditentukan oleh undang-undang otorisasi, peraturan, atau kebijakan pemerintah untuk kategori CUI yang tercantum dalam Registry CUI.

Persyaratan berlaku untuk semua komponen sistem dan organisasi non-federal yang memproses, menyimpan, atau mengirimkan CUI, atau memberikan perlindungan keamanan untuk komponen. Untuk informasi lebih lanjut, lihat NIST SP 800-171 Rev. 2 di Pusat Sumber Daya Keamanan Kom puter NIST.

AWS Security Hub CSPM menyediakan kontrol keamanan yang mendukung subset persyaratan NIST SP 800-171 Revisi 2. Kontrol melakukan pemeriksaan keamanan otomatis untuk sumber Layanan AWS daya tertentu. Untuk mengaktifkan dan mengelola kontrol ini, Anda dapat mengaktifkan kerangka kerja NIST SP 800-171 Revisi 2 sebagai standar di Security Hub CSPM. Perhatikan bahwa kontrol tidak mendukung persyaratan NIST SP 800-171 Revisi 2 yang memerlukan pemeriksaan manual.

Topik

- Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar
- Menentukan kontrol mana yang berlaku untuk standar

Mengkonfigurasi perekaman sumber daya untuk kontrol yang berlaku untuk standar

Untuk mengoptimalkan cakupan dan keakuratan temuan, penting untuk mengaktifkan dan mengkonfigurasi perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar NIST SP 800-171 Revisi 2 di AWS Security Hub CSPM. Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis AWS sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Jika tidak, Security Hub CSPM mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku untuk standar.

Untuk informasi tentang cara Security Hub CSPM menggunakan perekaman sumber daya di AWS Config, lihat. Mengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM Untuk informasi tentang mengonfigurasi perekaman sumber daya di AWS Config, lihat Bek erja dengan perekam konfigurasi di Panduan AWS Config Pengembang.

Tabel berikut menentukan jenis sumber daya yang akan direkam untuk kontrol yang berlaku untuk standar NIST SP 800-171 Revisi 2 di Security Hub CSPM.

Layanan AWS	Jenis sumber daya
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`

Layanan AWS	Jenis sumber daya
Awan Komputasi Elastis Amazon (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Layanan Penyimpanan Sederhana Amazon (Amazon S3)	`AWS::S3::Bucket`
Layanan Pemberitahuan Sederhana Amazon (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Menentukan kontrol mana yang berlaku untuk standar

Daftar berikut menentukan kontrol yang mendukung persyaratan NIST SP 800-171 Revisi 2 dan berlaku untuk standar NIST SP 800-171 Revisi 2 di AWS Security Hub CSPM. Untuk detail tentang persyaratan spesifik yang didukung kontrol, pilih kontrol. Kemudian lihat bidang Persyaratan terkait di detail untuk kontrol. Bidang ini menentukan setiap persyaratan NIST yang didukung kontrol. Jika bidang tidak menentukan persyaratan NIST tertentu, kontrol tidak mendukung persyaratan tersebut.

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
- [CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan
- [CloudTrail.4] validasi file CloudTrail log harus diaktifkan
- [CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
- [CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah
- [CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM
- [CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi
- [CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi
- [CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan
- [CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
- [CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi
- [CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
- [CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
- [CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan
- [CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
- [CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC
- [CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi
- [EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22
- [EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus
- [EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi
- [EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi

- [EC2.20] Kedua terowongan VPN untuk AWS Site-to-Site Koneksi VPN harus aktif
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki kekuatan AWS Config urasi
- [GuardDuty.1] GuardDuty harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS
- [S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS
- [S3.9] Bucket tujuan umum S3 harus mengaktifkan logging akses server
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.14] Bucket tujuan umum S3 harus mengaktifkan pembuatan versi
- [S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys
- [SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakanAWS KMS
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik

PCI DSS di Hub Keamanan CSPM

Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) adalah kerangka kerja kepatuhan pihak ketiga yang menyediakan seperangkat aturan dan pedoman untuk menangani informasi kartu kredit dan debit dengan aman. Dewan Standar Keamanan PCI (SSC) membuat dan memperbarui kerangka kerja ini.

AWS Security Hub CSPM menyediakan standar PCI DSS yang dapat membantu Anda tetap mematuhi kerangka kerja pihak ketiga ini. Anda dapat menggunakan standar ini untuk menemukan kerentanan keamanan dalam AWS sumber daya yang menangani data pemegang kartu. Sebaiknya aktifkan standar ini Akun AWS yang memiliki sumber daya yang menyimpan, memproses, atau mengirimkan data pemegang kartu atau data otentikasi sensitif. Penilaian oleh PCI SSC memvalidasi standar ini.

Security Hub CSPM menawarkan dukungan untuk PCI DSS v3.2.1 dan PCI DSS v4.0.1. Sebaiknya gunakan v4.0.1 agar tetap mengikuti praktik terbaik keamanan. Anda dapat mengaktifkan kedua versi standar secara bersamaan. Untuk informasi tentang mengaktifkan standar, lihatMengaktifkan standar keamanan. Jika saat ini Anda menggunakan v3.2.1 tetapi hanya ingin menggunakan v4.0.1, aktifkan versi yang lebih baru sebelum menonaktifkan versi yang lebih lama. Ini mencegah celah dalam

pemeriksaan keamanan Anda. Jika Anda menggunakan integrasi Security Hub CSPM dengan AWS Organizations dan ingin mengaktifkan batch v4.0.1 di beberapa akun, sebaiknya gunakan konfigurasi ??? pusat untuk melakukannya.

Bagian berikut menentukan kontrol mana yang berlaku untuk PCI DSS v3.2.1 dan PCI DSS v4.0.1.

Kontrol yang berlaku untuk PCI DSS v3.2.1

Daftar berikut menentukan kontrol CSPM Security Hub mana yang berlaku untuk PCI DSS v3.2.1. Untuk meninjau detail kontrol, pilih kontrol.

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

[EC2.1] Snapshot Amazon EBS tidak boleh dikonfigurasi agar dapat dipulihkan secara publik

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

[EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

[ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik

[GuardDuty.1] GuardDuty harus diaktifkan

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

[KMS.4]AWS KMSrotasi kunci harus diaktifkan

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

[Lambda.3] Fungsi lambda harus dalam VPC

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

[Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik

[RDS.1] Snapshot RDS harus bersifat pribadi

[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS

[S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah

[SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung

[SSM.1] Instans Amazon EC2 harus dikelola olehAWS Systems Manager

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

Kontrol yang berlaku untuk PCI DSS v4.0.1

Daftar berikut menentukan kontrol CSPM Security Hub yang berlaku untuk PCI DSS v4.0.1. Untuk meninjau detail kontrol, pilih kontrol.

[ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu

[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

[APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages

[AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan

[AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)

[Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

[CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

[CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada

[CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit

Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging

[CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

[CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas

[CodeBuild.3] CodeBuild Log S3 harus dienkripsi

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM

[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

[DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS

[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

[DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging

[DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging

[DMS.9] Titik akhir DMS harus menggunakan SSL

[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22

[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389

[EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik

[EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

[EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)

[EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389

[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan

[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

[EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh

[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

[ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru

[ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik

[ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis

[ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

[EFS.4] Titik akses EFS harus menegakkan identitas pengguna

[EKS.1] Titik akhir cluster EKS tidak boleh diakses publik

[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung

[EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi

[EKS.8] Cluster EKS harus mengaktifkan logging audit

[ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis

[ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan

[ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH

[ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

[ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

[ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

[ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS

[ELB.4] Application Load Balancer harus dikonfigurasi untuk menghapus header http yang tidak valid

[ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki kekuatan AWS Config urasi

[EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik

[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan

[ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik

[ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

[ES.5] Domain Elasticsearch harus mengaktifkan logging audit

[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

[GuardDuty.1] GuardDuty harus diaktifkan

[GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan

[GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan

[GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan

[GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

[IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus

[IAM.9] MFA harus diaktifkan untuk pengguna root

[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang

[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan

[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

[Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan

[Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan

[Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan

[Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan

[KMS.4]AWS KMSrotasi kunci harus diaktifkan

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung

[MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch

[MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker

[MSK.3] Konektor MSK Connect harus dienkripsi saat transit

[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch

[Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik

[Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru

[Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

[RDS.13] Upgrade versi minor otomatis RDS harus diaktifkan

[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

[RDS.20] Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting

[RDS.21] Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting

[RDS.22] Langganan notifikasi peristiwa RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting

[RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus

[RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log

[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

[RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch

[RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch

[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi

[Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit

[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit

[Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock

[S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys

[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok

[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek

[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek

[S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

[S3.9] Bucket tujuan umum S3 harus mengaktifkan logging akses server

[SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung

[SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis

[SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar

[SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging

[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

[WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan

[WAF.11]AWS WAFpencatatan ACL web harus diaktifkan

Service-managed standar dalam Security Hub CSPM

Standar yang dikelola layanan adalah standar keamanan yang dikelola orang lain Layanan AWS tetapi dapat Anda lihat di Security Hub CSPM. Misalnya, Service-Managed Standar: AWS Control Tower adalah standar yang dikelola layanan yang AWS Control Tower mengelola. Standar yang dikelola layanan berbeda dari standar keamanan yang dikelola AWS Security Hub CSPM dengan cara berikut:

- Pembuatan dan penghapusan standar — Anda membuat dan menghapus standar yang dikelola layanan dengan konsol atau API layanan pengelolaan, atau dengan. AWS CLI Sampai Anda membuat standar di layanan pengelolaan dengan salah satu cara tersebut, standar tidak muncul di konsol CSPM Hub Keamanan dan tidak dapat diakses oleh Security Hub CSPM API atau. AWS CLI
- Tidak ada pengaktifan kontrol secara otomatis — Saat Anda membuat standar yang dikelola layanan, Security Hub CSPM dan layanan pengelolaan tidak secara otomatis mengaktifkan kontrol yang berlaku untuk standar. Selain itu, ketika Security Hub CSPM merilis kontrol baru untuk standar, kontrol tersebut tidak diaktifkan secara otomatis. Ini adalah penyimpangan dari standar yang dikelola Security Hub CSPM. Untuk informasi selengkapnya tentang cara biasa mengonfigurasi kontrol di Security Hub CSPM, lihat. Memahami kontrol keamanan di Security Hub CSPM
- Mengaktifkan dan menonaktifkan kontrol — Sebaiknya aktifkan dan menonaktifkan kontrol di layanan pengelolaan untuk menghindari penyimpangan.
- Ketersediaan kontrol — Layanan pengelolaan memilih kontrol mana yang tersedia sebagai bagian dari standar yang dikelola layanan. Kontrol yang tersedia dapat mencakup semua, atau sebagian dari, kontrol CSPM Security Hub yang ada.

Setelah layanan pengelolaan membuat standar yang dikelola layanan dan menyediakan kontrol untuk itu, Anda dapat mengakses temuan kontrol, status kontrol, dan skor keamanan standar di konsol CSPM Hub Keamanan, API CSPM Hub Keamanan, atau. AWS CLI Beberapa atau semua informasi ini mungkin juga tersedia di layanan pengelolaan.

Pilih standar yang dikelola layanan dari daftar berikut untuk melihat detail selengkapnya.

Service-managed standar

- Service-Managed Standar: AWS Control Tower

Service-Managed Standar: AWS Control Tower

Bagian ini memberikan informasi tentang Service-Managed Standar: AWS Control Tower.

Apa itu Service-Managed Standar: AWS Control Tower?

Service-Managed Standar: AWS Control Tower adalah standar yang dikelola layanan yang AWS Control Tower mengelola yang mendukung subset kontrol Hub Keamanan. Standar ini dirancang untuk pengguna AWS Security Hub CSPM dan. AWS Control Tower Ini memungkinkan Anda mengonfigurasi kontrol detektif Security Hub CSPM dari layanan. AWS Control Tower

Kontrol detektif mendeteksi ketidakpatuhan sumber daya (misalnya, kesalahan konfigurasi) di dalam Anda. Akun AWS

> **Tip**
>
> Service-managed standar berbeda dari standar yang dikelola AWS Security Hub CSPM. Misalnya, Anda harus membuat dan menghapus standar yang dikelola layanan di layanan pengelolaan. Untuk informasi selengkapnya, lihat Service-managed standar dalam Security Hub CSPM.

Saat Anda mengaktifkan kontrol CSPM Security Hub AWS Control Tower, Control Tower juga mengaktifkan Security Hub CSPM untuk Anda di akun dan Wilayah tertentu, jika belum diaktifkan. Di konsol dan API Security Hub CSPM, Anda dapat melihat Service-Managed Standar: AWS Control Tower bersama standar Security Hub CSPM lainnya, setelah standar diaktifkan dari. AWS Control Tower

Untuk informasi selengkapnya tentang standar ini, lihat Kontrol CSPM Hub Keamanan di Panduan AWS Control Tower Pengguna.

Menciptakan standar

Standar ini tersedia di Security Hub CSPM hanya jika Anda mengaktifkan kontrol CSPM Hub Keamanan dari. AWS Control Tower AWS Control Tower membuat standar saat Anda pertama kali mengaktifkan kontrol yang berlaku dengan menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil `EnableControl` API)
- AWS CLI (jalankan `enable-control` perintah)

Saat Anda mengaktifkan kontrol CSPM Hub Keamanan melalui AWS Control Tower, jika Anda belum mengaktifkan CSPM Hub Keamanan, AWS Control Tower juga mengaktifkan CSPM Hub Keamanan untuk Anda di akun dan Wilayah tertentu tersebut.

Untuk mengidentifikasi kontrol CSPM Hub Keamanan berdasarkan ID kontrol di Katalog Kontrol, Anda dapat menggunakan bidang `Implementation.Identifier` di. AWS Control Tower Bidang ini dipetakan ke ID kontrol CSPM Security Hub dan dapat digunakan untuk memfilter ID kontrol tertentu. Untuk mengambil metadata kontrol untuk kontrol CSPM Security Hub tertentu (katakanlah, "CodeBuild.1“) di AWS Control Tower, Anda dapat menggunakan API: `ListControls`

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Anda tidak dapat melihat atau mengakses standar ini di konsol CSPM Security Hub, Security Hub CSPM API, atau AWS CLI tanpa terlebih dahulu menyiapkan AWS Control Tower dan mengaktifkan kontrol CSPM Security Hub agar tidak AWS Control Tower menggunakan salah satu metode sebelumnya.

Standar ini hanya tersedia di Wilayah AWS tempat AWS Control Tower yang tersedia.

Mengaktifkan dan menonaktifkan kontrol dalam standar

Setelah Anda mengaktifkan kontrol CSPM Security Hub AWS Control Tower dan Standar: Service-Managed AWS Control Tower standar telah dibuat, Anda dapat melihat standar dan kontrol yang tersedia di Security Hub CSPM.

Ketika Security Hub CSPM menambahkan kontrol baru ke Service-Managed Standar: AWS Control Tower standar, kontrol tersebut tidak secara otomatis diaktifkan untuk pelanggan yang mengaktifkan standar. Anda harus mengaktifkan dan menonaktifkan kontrol untuk standar AWS Control Tower dengan menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil `EnableControl` dan `DisableControl` API)
- AWS CLI (jalankan `disable-control` perintah `enable-control` dan)

Saat Anda mengubah status pengaktifan kontrol di AWS Control Tower, perubahan tersebut juga tercermin dalam CSPM Hub Keamanan.

Namun, menonaktifkan kontrol di Security Hub CSPM yang diaktifkan menghasilkan penyimp AWS Control Tower angan kontrol. Status kontrol di AWS Control Tower ditampilkan sebagai`Drifted`. Anda dapat mengatasi penyimpangan ini dengan menggunakan ResetEnabledControl API untuk mengatur ulang kontrol yang sedang menyimpang, atau dengan memilih Re-register OU di AWS Control Tower konsol, atau dengan menonaktifkan dan mengaktifkan kembali kontrol dalam AWS Control Tower menggunakan salah satu metode sebelumnya.

Menyelesaikan tindakan pemberdayaan dan penonaktifan AWS Control Tower membantu Anda menghindari penyimpangan kontrol.

Saat Anda mengaktifkan atau menonaktifkan kontrol di AWS Control Tower, tindakan tersebut berlaku di seluruh akun dan Wilayah yang diatur oleh AWS Control Tower. Jika Anda mengaktifkan dan menonaktifkan kontrol di Security Hub CSPM (tidak disarankan untuk standar ini), tindakan hanya berlaku untuk akun dan wilayah saat ini.

> **Note**
>
> Konfigurasi pusat tidak dapat digunakan untuk mengelola Service-Managed Standar: AWS Control Tower. Anda hanya dapat menggunakan AWS Control Tower layanan untuk mengaktifkan dan menonaktifkan kontrol dalam standar ini.

Melihat status pengaktifan dan status kontrol

Anda dapat melihat status pengaktifan suatu kontrol dengan menggunakan salah satu metode berikut:

- Konsol CSPM Hub Keamanan, API CSPM Hub Keamanan, atau AWS CLI
- AWS Control Tower konsol
- AWS Control Tower API untuk melihat daftar kontrol yang diaktifkan (panggil `ListEnabledControls` API)
- AWS CLI untuk melihat daftar kontrol yang diaktifkan (jalankan `list-enabled-controls` perintah)

Kontrol yang Anda nonaktifkan AWS Control Tower memiliki status pengaktifan di CSPM Hub Keamanan kecuali jika Anda secara eksplisit mengaktifkan kontrol tersebut di CSPM Hub Keamanan. `Disabled`

Security Hub CSPM menghitung status kontrol berdasarkan status alur kerja dan status kepatuhan dari temuan kontrol. Untuk informasi selengkapnya tentang status pengaktifan dan status kontrol, lihat. Meninjau detail kontrol di Security Hub CSPM

Berdasarkan status kontrol, Security Hub CSPM menghitung skor keamanan untuk Service-Managed Standar:. AWS Control Tower Skor ini hanya tersedia di Security Hub CSPM. Selain itu, Anda hanya dapat melihat temuan kontrol di Security Hub CSPM. Skor keamanan standar dan temuan kontrol tidak tersedia di AWS Control Tower.

> **Note**
>
> Saat Anda mengaktifkan kontrol untuk Service-Managed Standar: AWS Control Tower, Security Hub CSPM mungkin memerlukan waktu hingga 18 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan terkait layanan yang ada AWS Config . Anda mungkin memiliki aturan terkait layanan yang ada jika Anda telah mengaktifkan standar dan kontrol lain di Security Hub CSPM. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Menghapus standar

Anda dapat menghapus standar yang dikelola layanan ini AWS Control Tower dengan menonaktifkan semua kontrol yang berlaku menggunakan salah satu metode berikut:

- AWS Control Tower konsol
- AWS Control Tower API (panggil `DisableControl` API)
- AWS CLI (jalankan `disable-control` perintah)

Menonaktifkan semua kontrol akan menghapus standar di semua akun terkelola dan Wilayah yang diatur di AWS Control Tower. Menghapus standar di AWS Control Tower menghapusnya dari halaman Standar konsol CSPM Hub Keamanan, dan Anda tidak dapat lagi mengaksesnya dengan menggunakan Security Hub CSPM API atau. AWS CLI

> **Note**
>
> Menonaktifkan semua kontrol dari standar di Security Hub CSPM tidak menonaktifkan atau menghapus standar.

Menonaktifkan layanan Security Hub CSPM akan menghapus Service-Managed Standar: AWS Control Tower dan standar lainnya yang telah Anda aktifkan.

Menemukan format bidang untuk Service-Managed Standar: AWS Control Tower

Saat Anda membuat Service-Managed Standar: AWS Control Tower dan mengaktifkan kontrol untuk itu, Anda akan mulai menerima temuan kontrol di Security Hub CSPM. Security Hub CSPM melaporkan temuan kontrol di. AWS Format Penemuan Keamanan (ASFF) Ini adalah nilai ASFF untuk Nama Sumber Daya Amazon (ARN) standar ini dan: `GeneratorId`

- ARN Standar — *`arn:aws:us-east-1`*`:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId – `service-managed-aws-control-tower/v/1.0.0/`*`CodeBuild.1`*

Untuk temuan sampel untuk Service-Managed Standar: AWS Control Tower, lihatSampel temuan kontrol.

Kontrol yang berlaku untuk Service-Managed Standar: AWS Control Tower

Service-Managed Standar: AWS Control Tower mendukung subset kontrol yang merupakan bagian dari standar F AWS oundational Security Best Practices (FSBP). Pilih kontrol untuk melihat informasi tentangnya, termasuk langkah-langkah remediasi untuk temuan yang gagal.

Untuk melihat kontrol CSPM Hub Keamanan yang didukung oleh AWS Control Tower, Anda dapat menggunakan salah satu metode berikut:

- AWS Kontrol konsol Katalog tempat Anda dapat memfilter "`Control owner = AWS Security Hub`"
- AWS Kontrol Katalog API (panggil `ListControls` API) dengan filter `Implementations` untuk `Types` diperiksa `AWS::SecurityHub::SecurityControl`
- AWS CLI (jalankan `list-controls` perintah) dengan filter untuk`Implementations`. Contoh perintah CLI:

  ```
  aws controlcatalog list-controls --filter '{"Implementations":{"Types":["AWS::SecurityHub::SecurityControl"]}}'
  ```

Batas regional pada kontrol CSPM Hub Keamanan saat diaktifkan melalui standar Menara Kontrol mungkin tidak sesuai dengan batas Regional pada kontrol yang mendasarinya.

Di Security Hub CSPM, jika temuan kontrol konsolidasi dimatikan di akun Anda, `ProductFields.ControlId` bidang dalam temuan yang dihasilkan menggunakan ID kontrol berbasis standar. ID kontrol berbasis standar diformat sebagai CT. ***`ControlId`***(misalnya, CT.CodeBuild.1).

Untuk informasi selengkapnya tentang standar ini, lihat Kontrol CSPM Hub Keamanan di Panduan AWS Control Tower Pengguna.

Mengaktifkan standar keamanan

Saat Anda mengaktifkan standar keamanan di AWS Security Hub CSPM, Security Hub CSPM secara otomatis membuat dan mengaktifkan semua kontrol yang berlaku untuk standar. Security Hub CSPM juga mulai menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk kontrol.

Untuk mengoptimalkan cakupan dan keakuratan temuan, aktifkan dan konfigurasikan perekaman sumber daya AWS Config sebelum Anda mengaktifkan standar. Saat Anda mengonfigurasi perekaman sumber daya, pastikan juga untuk mengaktifkannya untuk semua jenis sumber daya yang diperiksa oleh kontrol yang berlaku untuk standar. Jika tidak, Security Hub CSPM mungkin tidak dapat mengevaluasi sumber daya yang sesuai, dan menghasilkan temuan akurat untuk kontrol yang berlaku untuk standar. Untuk informasi selengkapnya, lihat Mengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM.

Standar keamanan Multicloud, seperti CIS Azure Foundations Benchmark v4.0.0, memiliki persyaratan yang berbeda dari standar. AWS Standar Multicloud memerlukan konektor CSPM Security Hub untuk penyedia cloud eksternal dan tidak mengharuskan Anda untuk mengkonfigurasi AWS Config atau membuat perekam konfigurasi secara manual. Konektor multicloud Security Hub CSPM secara otomatis menyiapkan perekam terkait layanan untuk mengevaluasi sumber daya di lingkungan cloud eksternal.

Setelah mengaktifkan standar, Anda dapat menonaktifkan atau mengaktifkan kembali kontrol individual yang berlaku untuk standar. Jika Anda menonaktifkan kontrol untuk standar, Security Hub CSPM berhenti menghasilkan temuan untuk kontrol tersebut. Selain itu, Security Hub CSPM mengabaikan kontrol saat menghitung skor keamanan untuk standar. Skor keamanan adalah persentase kontrol yang lulus evaluasi, relatif terhadap jumlah total kontrol yang berlaku untuk standar, diaktifkan, dan memiliki data evaluasi.

Saat Anda mengaktifkan standar, Security Hub CSPM menghasilkan skor keamanan awal untuk standar tersebut, biasanya dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ring kasan atau Standar Keamanan di konsol CSPM Hub Keamanan. Skor keamanan dibuat

hanya untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut di konsol. Selain itu, perekaman sumber daya harus dikonfigurasi agar skor muncul. AWS Config Di Wilayah China dan AWS GovCloud (US) Regions, dibutuhkan waktu hingga 24 jam bagi Security Hub CSPM untuk menghasilkan skor keamanan awal untuk standar. Setelah Security Hub CSPM menghasilkan skor awal, itu memperbarui skor setiap 24 jam. Untuk menentukan kapan skor keamanan terakhir diperbarui, Anda dapat merujuk ke stempel waktu yang disediakan oleh Security Hub CSPM untuk skor tersebut. Untuk informasi selengkapnya, lihat Menghitung skor keamanan.

Cara Anda mengaktifkan standar tergantung pada apakah Anda menggunakan konfigurasi pusat untuk mengelola Security Hub CSPM untuk beberapa akun dan. Wilayah AWS Sebaiknya gunakan konfigurasi pusat jika Anda ingin mengaktifkan standar di lingkungan multi-akun, Multi-wilayah. Anda dapat menggunakan konfigurasi pusat jika Anda mengintegrasikan Security Hub CSPM dengan. AWS Organizations Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengaktifkan setiap standar secara terpisah di setiap akun dan setiap Wilayah.

Topik

- Mengaktifkan standar di beberapa akun dan Wilayah AWS
- Mengaktifkan standar dalam satu akun dan Wilayah AWS
- Memeriksa status standar

Mengaktifkan standar di beberapa akun dan Wilayah AWS

Untuk mengaktifkan dan mengonfigurasi standar keamanan di beberapa akun dan Wilayah AWS, gunakan konfigurasi pusat. Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang mengaktifkan satu atau lebih standar. Administrator kemudian dapat mengaitkan kebijakan konfigurasi dengan akun individual, unit organisasi (OU), atau root. Kebijakan konfigurasi memengaruhi Wilayah asal, juga disebut sebagai Wilayah agregasi, dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan opsi penyesuaian. Misalnya, Anda dapat memilih untuk mengaktifkan hanya standar Praktik AWS Terbaik Keamanan Dasar (FSBP) untuk satu OU. Untuk OU lain, Anda dapat memilih untuk mengaktifkan standar FSBP dan standar Center for Internet Security (CIS) Foun AWS dations Benchmark v1.4.0. Untuk informasi tentang membuat kebijakan konfigurasi yang mengaktifkan standar tertentu yang Anda tentukan, lihatMembuat dan mengaitkan kebijakan konfigurasi.

Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM tidak secara otomatis mengaktifkan standar apa pun di akun baru atau yang sudah ada. Sebagai gantinya, administrator CSPM Hub

Keamanan menentukan standar mana yang akan diaktifkan di akun yang berbeda saat mereka membuat kebijakan konfigurasi CSPM Hub Keamanan untuk organisasi mereka. Security Hub CSPM menawarkan kebijakan konfigurasi yang direkomendasikan di mana hanya standar FSBP yang diaktifkan. Untuk informasi selengkapnya, lihat Jenis kebijakan konfigurasi.

> **Note**
>
> Administrator Security Hub CSPM dapat menggunakan kebijakan konfigurasi untuk mengaktifkan standar apa pun kecuali standar yang dikelola layanan AWS Control Tower . Untuk mengaktifkan standar ini, administrator harus menggunakan AWS Control Tower secara langsung. Mereka juga harus digunakan AWS Control Tower untuk mengaktifkan atau menonaktifkan kontrol individual dalam standar ini untuk akun yang dikelola secara terpusat.

Jika Anda ingin beberapa akun mengaktifkan dan mengonfigurasi standar untuk akunnya sendiri, administrator CSPM Hub Keamanan dapat menetapkan akun tersebut sebagai akun yang dikelola sendiri. Self-managed akun harus mengaktifkan dan mengkonfigurasi standar secara terpisah di setiap Wilayah.

Mengaktifkan standar dalam satu akun dan Wilayah AWS

Jika Anda tidak menggunakan konfigurasi pusat atau Anda memiliki akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk mengaktifkan standar keamanan secara terpusat di beberapa akun atau Wilayah AWS. Namun, Anda dapat mengaktifkan standar dalam satu akun dan Wilayah. Anda dapat melakukan ini dengan menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Security Hub CSPM console

Ikuti langkah-langkah berikut untuk mengaktifkan standar dalam satu akun dan Wilayah dengan menggunakan konsol CSPM Security Hub.

Untuk mengaktifkan standar dalam satu akun dan Wilayah

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Dengan menggunakan Wilayah AWS pemilih di sudut kanan atas halaman, pilih Wilayah tempat Anda ingin mengaktifkan standar.
3. Di panel navigasi, pilih Standar keamanan. Halaman Standar keamanan mencantumkan semua standar yang didukung Security Hub CSPM saat ini. Jika Anda sudah mengaktifkan

standar, bagian untuk standar mencakup skor keamanan saat ini dan detail tambahan untuk standar tersebut.

4. Di bagian untuk standar yang ingin Anda aktifkan, pilih Aktifkan standar.

Untuk mengaktifkan standar di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

Security Hub CSPM API

Untuk mengaktifkan standar secara terprogram dalam satu akun dan Wilayah, gunakan operasi. BatchEnableStandards Atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan batch-enable-standards perintah.

Dalam permintaan Anda, gunakan `StandardsArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda aktifkan. Juga tentukan Wilayah tempat permintaan Anda berlaku. Misalnya, perintah berikut mengaktifkan standar F AWS oundational Security Best Practices (FSBP):

```
$ aws securityhub batch-enable-standards \
--standards-subscription-requests '{"StandardsArn":"arn:aws:securityhub:us-
east-1::standards/aws-foundational-security-best-practices/v/1.0.0"}' \
--region us-east-1
```

Di *arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0* mana ARN standar FSBP di Wilayah Timur AS (Virginia Utara), dan *us-east-1* merupakan Wilayah di mana untuk mengaktifkannya.

Untuk mendapatkan ARN untuk standar, gunakan DescribeStandards operasi atau, jika Anda menggunakan AWS CLI, jalankan describe-standards perintah.

Untuk terlebih dahulu meninjau daftar standar yang saat ini diaktifkan di akun Anda, Anda dapat menggunakan GetEnabledStandards operasi. Jika Anda menggunakan AWS CLI, Anda dapat menjalankan perintah get-enabled-standards untuk mengambil daftar ini.

Setelah Anda mengaktifkan standar, Security Hub CSPM mulai melakukan tugas untuk mengaktifkan standar di akun dan Wilayah yang ditentukan. Ini termasuk membuat semua kontrol yang berlaku untuk standar. Untuk memantau status tugas-tugas ini, Anda dapat memeriksa status standar untuk akun dan Wilayah.

Memeriksa status standar

Saat Anda mengaktifkan standar keamanan untuk akun, Security Hub CSPM mulai membuat semua kontrol yang berlaku untuk standar di akun. Security Hub CSPM juga melakukan tugas tambahan untuk mengaktifkan standar untuk akun, seperti menghasilkan skor keamanan awal untuk standar. Sementara Security Hub CSPM melakukan tugas-tugas ini, status standar adalah Pending untuk akun. Status standar kemudian melewati status tambahan, yang dapat Anda pantau dan periksa.

> **Note**
>
> Perubahan pada kontrol individu untuk standar tidak mempengaruhi status standar secara keseluruhan. Misalnya, jika Anda mengaktifkan kontrol yang sebelumnya dinonaktifkan, perubahan Anda tidak memengaruhi status standar. Demikian pula, jika Anda mengubah nilai parameter untuk kontrol yang diaktifkan, perubahan Anda tidak memengaruhi status standar.

Untuk memeriksa status standar dengan menggunakan konsol CSPM Security Hub, pilih Standar keamanan di panel navigasi. Halaman Standar keamanan mencantumkan semua standar yang didukung Security Hub CSPM saat ini. Jika Security Hub CSPM saat ini melakukan tugas untuk mengaktifkan standar, bagian untuk standar menunjukkan bahwa Security Hub CSPM masih menghasilkan skor keamanan untuk standar. Jika standar diaktifkan, bagian untuk standar menyertakan skor saat ini. Pilih Lihat hasil untuk meninjau detail tambahan, termasuk status kontrol individual yang berlaku untuk standar. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Untuk memeriksa status standar secara terprogram dengan Security Hub CSPM API, gunakan operasi. GetEnabledStandards Dalam permintaan Anda, secara opsional gunakan `StandardsSubscriptionArns` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari standar yang statusnya ingin Anda periksa. Jika Anda menggunakan AWS Command Line Interface (AWS CLI), Anda dapat menjalankan perintah get-enabled-standards untuk memeriksa status standar. Untuk menentukan ARN standar untuk diperiksa, gunakan `standards-subscription-arns` parameter. Untuk menentukan ARN mana yang akan ditentukan, Anda dapat menggunakan DescribeStandards operasi atau, untuk AWS CLI, menjalankan describe-standards perintah.

Jika permintaan Anda berhasil, Security Hub CSPM merespons dengan array objek. `StandardsSubscription` Lang ganan standar adalah AWS sumber daya yang dibuat oleh Security Hub CSPM di akun saat standar diaktifkan untuk akun tersebut. Setiap

`StandardsSubscription` objek memberikan detail tentang standar yang saat ini diaktifkan atau sedang diaktifkan atau dinonaktifkan untuk akun. Dalam setiap objek, `StandardsStatus` bidang menentukan status standar saat ini untuk akun.

Status standar (`StandardsStatus`) dapat menjadi salah satu dari berikut ini.

PENDING

Security Hub CSPM saat ini sedang melakukan tugas untuk mengaktifkan standar untuk akun. Ini termasuk membuat kontrol yang berlaku untuk standar, dan menghasilkan skor keamanan awal untuk standar. Diperlukan beberapa menit bagi Security Hub CSPM untuk menyelesaikan semua tugas. Standar juga dapat memiliki status ini jika sudah diaktifkan untuk akun dan Security Hub CSPM saat ini menambahkan kontrol baru ke standar.

Jika standar memiliki status ini, Anda mungkin tidak dapat mengambil detail kontrol individual yang berlaku untuk standar. Selain itu, Anda mungkin tidak dapat mengonfigurasi atau menonaktifkan kontrol individual untuk standar. Misalnya, jika Anda mencoba menonaktifkan kontrol dengan menggunakan UpdateStandardsControl operasi, kesalahan terjadi.

Untuk menentukan apakah Anda dapat mengonfigurasi atau mengelola kontrol individual untuk standar, lihat nilai untuk `StandardsControlsUpdatable` bidang tersebut. Jika nilai untuk bidang ini adalah`READY_FOR_UPDATES`, Anda dapat mulai mengelola kontrol individual untuk standar. Jika tidak, tunggu hingga Security Hub CSPM menyelesaikan tugas pemrosesan tambahan untuk mengaktifkan standar.

READY

Standar saat ini diaktifkan untuk akun. Security Hub CSPM dapat menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk semua kontrol yang berlaku untuk standar dan saat ini diaktifkan. Security Hub CSPM juga dapat menghitung skor keamanan untuk standar.

Jika standar memiliki status ini, Anda dapat mengambil rincian kontrol individual yang berlaku untuk standar. Selain itu, Anda dapat mengonfigurasi, menonaktifkan, atau mengaktifkan kembali kontrol. Anda juga dapat menonaktifkan standar.

INCOMPLETE

Security Hub CSPM tidak dapat mengaktifkan standar sepenuhnya untuk akun. Security Hub CSPM tidak dapat menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk semua kontrol yang berlaku untuk standar dan saat ini diaktifkan. Selain itu, Security Hub CSPM tidak dapat menghitung skor keamanan untuk standar.

Untuk standar multicloud, langganan masuk `INCOMPLETE` dengan alasan status `NO_AVAILABLE_MULTICLOUD_CONNECTOR` jika Anda mengaktifkan standar tanpa konektor CSPM. Langganan secara otomatis `READY` beralih ke saat konektor tersedia.

Untuk menentukan mengapa standar tidak dapat diaktifkan sepenuhnya, lihat informasi dalam `StandardsStatusReason` array. Array ini menentukan masalah yang mencegah Security Hub CSPM mengaktifkan standar. Jika terjadi kesalahan internal, coba aktifkan standar untuk akun lagi. Untuk jenis masalah lainnya, periksa AWS Config pengaturan Anda. Anda juga dapat menonaktifkan kontrol individual yang tidak ingin Anda periksa, atau menonaktifkan standar sepenuhnya.

DELETING

Security Hub CSPM saat ini sedang memproses permintaan untuk menonaktifkan standar untuk akun. Ini termasuk menonaktifkan kontrol yang berlaku untuk standar, dan menghapus skor keamanan terkait. Diperlukan beberapa menit bagi Security Hub CSPM untuk menyelesaikan pemrosesan permintaan.

Jika standar memiliki status ini, Anda tidak dapat mengaktifkan kembali standar atau mencoba menonaktifkannya lagi untuk akun tersebut. Security Hub CSPM harus menyelesaikan pemrosesan permintaan saat ini terlebih dahulu. Selain itu, Anda tidak dapat mengambil detail kontrol individual yang berlaku untuk standar atau mengelola kontrol.

FAILED

Security Hub CSPM tidak dapat menonaktifkan standar untuk akun. Satu atau lebih kesalahan terjadi ketika Security Hub CSPM mencoba menonaktifkan standar. Selain itu, Security Hub CSPM tidak dapat menghitung skor keamanan untuk standar.

Untuk menentukan mengapa standar tidak dinonaktifkan sepenuhnya, lihat informasi dalam `StandardsStatusReason` array. Array ini menentukan masalah yang mencegah Security Hub CSPM menonaktifkan standar.

Jika standar memiliki status ini, Anda tidak dapat mengambil detail kontrol individual yang berlaku untuk standar atau mengelola kontrol. Namun, Anda dapat mengaktifkan kembali standar untuk akun. Jika Anda mengatasi masalah yang mencegah Security Hub CSPM menonaktifkan standar, Anda juga dapat mencoba menonaktifkan standar lagi.

Jika status standar adalah`READY`, Security Hub CSPM menjalankan pemeriksaan keamanan dan menghasilkan temuan untuk semua kontrol yang berlaku untuk standar dan saat ini diaktifkan. Untuk

status lain, Security Hub CSPM mungkin menjalankan pemeriksaan dan menghasilkan temuan untuk beberapa, tetapi tidak semua, kontrol yang diaktifkan. Diperlukan waktu hingga 24 jam untuk menghasilkan atau memperbarui temuan kontrol. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Meninjau detail standar keamanan

Setelah mengaktifkan standar keamanan di AWS Security Hub CSPM, Anda dapat menggunakan konsol untuk meninjau detail standar. Di konsol, halaman detail untuk standar mencakup informasi berikut:

- Skor keamanan saat ini untuk standar.
- Tabel kontrol yang berlaku untuk standar.
- Statistik agregat untuk kontrol yang berlaku untuk standar.
- Ringkasan visual dari status kontrol yang berlaku untuk standar.
- Ringkasan visual pemeriksaan keamanan untuk kontrol yang diaktifkan dan berlaku untuk standar. Jika Anda mengintegrasikan dengan AWS Organizations, kontrol yang diaktifkan di setidaknya satu akun organisasi dianggap diaktifkan.

Untuk meninjau detail ini, pilih Standar keamanan di panel navigasi di konsol. Kemudian, di bagian untuk standar, pilih Lihat hasil. Untuk analisis yang lebih mendalam, Anda dapat memfilter dan mengurutkan data, dan menelusuri ke bawah untuk meninjau detail kontrol individual yang berlaku untuk standar.

Topik

- Memahami skor keamanan standar
- Meninjau kontrol untuk standar

Memahami skor keamanan standar

Pada konsol CSPM AWS Security Hub, halaman detail untuk standar menampilkan skor keamanan untuk standar. Skor adalah persentase kontrol yang lulus evaluasi, relatif terhadap jumlah total kontrol yang berlaku untuk standar, diaktifkan, dan memiliki data evaluasi. Di bawah skor adalah bagan yang merangkum pemeriksaan keamanan untuk kontrol yang diaktifkan untuk standar. Ini termasuk jumlah pemeriksaan keamanan yang lulus dan gagal. Untuk akun administrator, skor dan bagan standar digabungkan di seluruh akun administrator dan semua akun anggota. Untuk meninjau

pemeriksaan keamanan yang gagal untuk kontrol yang memiliki tingkat keparahan tertentu, pilih tingkat keparahannya.

Saat Anda mengaktifkan standar, Security Hub CSPM menghasilkan skor keamanan awal untuk standar tersebut, biasanya dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ring kasan atau halaman Standar Keamanan di konsol CSPM Hub Keamanan. Skor dibuat hanya untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Di Wilayah China dan AWS GovCloud (US) Regions, dibutuhkan waktu hingga 24 jam bagi Security Hub CSPM untuk menghasilkan skor awal. Setelah Security Hub CSPM menghasilkan skor awal untuk standar, itu memperbarui skor setiap 24 jam. Untuk informasi selengkapnya, lihat Menghitung skor keamanan.

Semua data pada halaman detail standar keamanan spesifik untuk saat ini Wilayah AWS kecuali Anda menetapkan Wilayah agregasi. Jika Anda menetapkan Wilayah agregasi, skor keamanan berlaku di seluruh Wilayah dan menyertakan temuan untuk semua Wilayah yang ditautkan. Selain itu, status kepatuhan kontrol mencerminkan temuan dari Wilayah terkait, dan jumlah pemeriksaan keamanan mencakup temuan dari Wilayah terkait.

Meninjau kontrol untuk standar

Saat Anda menggunakan konsol CSPM AWS Security Hub untuk meninjau detail standar yang Anda aktifkan, Anda dapat meninjau tabel kontrol keamanan yang berlaku untuk standar. Untuk setiap kontrol, tabel mencakup informasi berikut:

- ID kontrol dan judul.
- Status kontrol. Untuk informasi selengkapnya, lihat Mengevaluasi status kepatuhan dan status kontrol.
- Tingkat keparahan yang diberikan pada kontrol.
- Jumlah cek yang gagal dan jumlah total cek. Jika berlaku, bidang Pemeriksaan Gagal juga menentukan jumlah temuan dengan status Tidak Diket ahui.
- Apakah kontrol mendukung parameter khusus. Untuk informasi selengkapnya, lihat Memahami parameter kontrol di Security Hub CSPM.

Security Hub CSPM memperbarui status kontrol dan jumlah pemeriksaan keamanan setiap 24 jam. Stempel waktu di bagian atas halaman menunjukkan kapan Security Hub CSPM terbaru memperbarui data ini.

Untuk akun administrator, status kontrol dan jumlah pemeriksaan keamanan digabungkan di seluruh akun administrator dan semua akun anggota. Jumlah kontrol yang diaktifkan mencakup kontrol yang diaktifkan untuk standar di akun administrator atau setidaknya satu akun anggota. Jumlah kontrol yang dinonaktifkan mencakup kontrol yang dinonaktifkan untuk standar di akun administrator dan semua akun anggota.

Anda dapat memfilter tabel kontrol yang berlaku untuk standar. Menggunakan opsi Filter berdasarkan di sebelah tabel, Anda dapat memilih untuk hanya melihat kontrol yang diaktifkan atau hanya dinonaktifkan untuk standar. Jika Anda hanya menampilkan kontrol yang diaktifkan, Anda dapat memfilter tabel lebih lanjut berdasarkan status kontrol. Anda kemudian dapat fokus pada kontrol yang memiliki status kontrol tertentu. Selain opsi Filter berdasarkan, Anda dapat memasukkan kriteria filter di kotak kontrol Filter. Misalnya, Anda dapat memfilter berdasarkan ID kontrol atau judul.

Pilih metode akses pilihan Anda. Kemudian ikuti langkah-langkah untuk meninjau kontrol yang berlaku untuk standar yang Anda aktifkan.

Security Hub CSPM console

Untuk meninjau kontrol untuk standar yang diaktifkan

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Standar keamanan di panel navigasi.
3. Di bagian untuk standar, pilih Lihat hasil.

Tabel di bagian bawah halaman mencantumkan semua kontrol yang berlaku untuk standar. Anda dapat memfilter dan mengurutkan tabel. Anda juga dapat mengunduh halaman tabel saat ini sebagai file CSV. Untuk melakukan ini, pilih Unduh di atas tabel. Jika Anda memfilter tabel, file yang diunduh hanya menyertakan kontrol yang sesuai dengan pengaturan filter Anda saat ini.

Security Hub CSPM API

Untuk meninjau kontrol untuk standar yang diaktifkan

1. Gunakan pen ListSecurityControlDefinitions goperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan perintah list-secur ity-control-definition.

   Tentukan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda tinjau kontrolnya. Untuk mendapatkan ARN untuk standar, gunakan DescribeStandards operasi atau jalankan

perintah describe-standards. Jika Anda tidak menentukan ARN untuk standar, Security Hub CSPM mengembalikan semua ID kontrol keamanan.

2. Gunakan pen ListStandardsControlAssociations goperasian Security Hub CSPM API, atau jalankan perintah list -standards-control-association. Operasi ini memberi tahu Anda standar mana kontrol diaktifkan.

   Identifikasi kontrol dengan memberikan ID kontrol keamanan atau ARN. Parameter paginasi bersifat opsional.

Contoh berikut memberi tahu Anda standar mana Config.1 kontrol diaktifkan.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

Mematikan standar keamanan yang diaktifkan secara otomatis

Jika organisasi Anda tidak menggunakan konfigurasi pusat, organisasi menggunakan jenis konfigurasi yang disebut konfigurasi lokal. Dengan konfigurasi lokal, AWS Security Hub CSPM dapat secara otomatis mengaktifkan standar keamanan default untuk akun anggota baru saat akun bergabung dengan organisasi Anda. Semua kontrol yang berlaku untuk standar default ini juga diaktifkan secara otomatis.

Saat ini, standar keamanan default adalah standar Prakti AWS k Terbaik Keamanan Dasar dan standar Center for Internet Security (CIS) Foun AWS dations Benchmark v1.2.0. Untuk informasi tentang standar ini, lihatReferensi standar untuk Security Hub CSPM.

Jika Anda lebih suka mengaktifkan standar keamanan secara manual untuk akun anggota baru, Anda dapat menonaktifkan pengaktifan otomatis standar default. Anda dapat melakukan ini hanya jika Anda mengintegrasikan dengan AWS Organizations dan menggunakan konfigurasi lokal. Jika Anda menggunakan konfigurasi pusat, Anda dapat membuat kebijakan konfigurasi yang mengaktifkan standar default dan mengaitkan kebijakan dengan root. Semua akun organisasi dan OU Anda kemudian mewarisi kebijakan konfigurasi ini kecuali jika dikaitkan dengan kebijakan yang berbeda atau dikelola sendiri. Jika Anda tidak mengintegrasikan AWS Organizations, Anda dapat menonaktifkan standar default saat pertama kali mengaktifkan Security Hub CSPM atau yang lebih baru. Untuk mempelajari caranya, lihat Menonaktifkan standar.

Untuk mematikan pengaktifan otomatis standar default untuk akun anggota baru, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Security Hub CSPM console

Ikuti langkah-langkah ini untuk mematikan pengaktifan otomatis standar default dengan menggunakan konsol CSPM Security Hub.

Untuk mematikan pengaktifan otomatis standar default

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredenSIAL akun administrator.
2. Di panel navigasi, di bawah Peng aturan, pilih Konfigurasi.
3. Di bagian I khtisar, pilih Edit.
4. Di bawah Pengaturan akun baru, kosongkan kotak centang Aktifkan standar keamanan default.
5. Pilih Konfirmasi.

Security Hub CSPM API

Untuk mematikan pengaktifan otomatis standar default secara terprogram, dari akun administrator CSPM Hub Keamanan, gunakan pen UpdateOrganizationConfiguration goperasian Security Hub CSPM API. Dalam permintaan Anda, tent `NONE` ukan untuk `AutoEnableStandards` parameter.

Jika Anda menggunakan AWS CLI, jalankan update-organization-configuration perintah untuk mematikan pengaktifan otomatis standar default. Untuk parameter `auto-enable-standards`, tentukan `NONE`. Misalnya, perintah berikut secara otomatis mengaktifkan Security Hub CSPM untuk akun anggota baru, dan mematikan pengaktifan otomatis standar default untuk akun tersebut.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

Menonaktifkan standar keamanan

Saat Anda menonaktifkan standar keamanan di AWS Security Hub CSPM, hal berikut terjadi:

- Semua kontrol yang berlaku untuk standar dinonaktifkan, kecuali jika terkait dengan standar lain yang saat ini diaktifkan.
- Pemeriksaan keamanan untuk kontrol yang dinonaktifkan tidak lagi dilakukan, dan tidak ada temuan tambahan yang dihasilkan untuk kontrol yang dinonaktifkan.
- Temuan yang ada untuk kontrol yang dinonaktifkan diarsipkan secara otomatis setelah sekitar 3-5 hari.
- AWS Config aturan yang dibuat oleh Security Hub CSPM untuk kontrol yang dinonaktifkan akan dihapus.

Penghapusan AWS Config aturan yang sesuai biasanya terjadi dalam beberapa menit setelah menonaktifkan standar. Namun, mungkin butuh waktu lebih lama. Jika permintaan pertama gagal menghapus aturan, Security Hub CSPM mencoba lagi setiap 12 jam. Namun, jika Anda menonaktifkan Security Hub CSPM atau tidak mengaktifkan standar lain, Security Hub CSPM tidak dapat mencoba lagi, yang berarti tidak dapat menghapus aturan. Jika ini terjadi dan Anda perlu menghapus aturan, hubungi AWS Dukungan.

Topik

- Menonaktifkan standar di beberapa akun dan Wilayah AWS
- Menonaktifkan standar dalam satu akun dan Wilayah AWS

Menonaktifkan standar di beberapa akun dan Wilayah AWS

Untuk menonaktifkan standar keamanan di beberapa akun dan Wilayah AWS, gunakan konfigurasi pusat. Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang menonaktifkan satu atau lebih standar. Administrator kemudian dapat mengaitkan kebijakan konfigurasi dengan akun individual, unit organisasi (OU), atau root. Kebijakan konfigurasi memengaruhi Wilayah asal, juga disebut sebagai Wilayah agregasi, dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan opsi penyesuaian. Misalnya, Anda dapat memilih untuk menonaktifkan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) dalam satu OU. Untuk OU lain, Anda dapat memilih untuk menonaktifkan PCI DSS dan National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 standar. Untuk informasi tentang membuat kebijakan konfigurasi yang mengaktifkan atau menonaktifkan standar individual yang Anda tentukan, lihatMembuat dan mengaitkan kebijakan konfigurasi.

> **Note**
>
> Administrator Security Hub CSPM dapat menggunakan kebijakan konfigurasi untuk menonaktifkan standar apa pun kecuali standar yang dikelola layanan AWS Control Tower . Untuk menonaktifkan standar ini, administrator harus menggunakan AWS Control Tower secara langsung. Mereka juga harus digunakan AWS Control Tower untuk menonaktifkan atau mengaktifkan kontrol individual dalam standar ini untuk akun yang dikelola secara terpusat.

Jika Anda ingin beberapa akun mengonfigurasi atau menonaktifkan standar untuk akunnya sendiri, administrator CSPM Hub Keamanan dapat menetapkan akun tersebut sebagai akun yang dikelola sendiri. Self-managed akun harus menonaktifkan standar secara terpisah di setiap Wilayah.

Menonaktifkan standar dalam satu akun dan Wilayah AWS

Jika Anda tidak menggunakan konfigurasi pusat atau Anda memiliki akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk menonaktifkan standar keamanan secara terpusat di beberapa akun atau Wilayah AWS. Namun, Anda dapat menonaktifkan standar dalam satu akun dan Wilayah. Anda dapat melakukan ini dengan menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Security Hub CSPM console

Ikuti langkah-langkah ini untuk menonaktifkan standar dalam satu akun dan Wilayah dengan menggunakan konsol CSPM Security Hub.

Untuk menonaktifkan standar dalam satu akun dan Wilayah

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Dengan menggunakan pem Wilayah AWS ilih di sudut kanan atas halaman, pilih Wilayah di mana Anda ingin menonaktifkan standar.
3. Di panel navigasi, pilih Standar keamanan.
4. Di bagian untuk standar yang ingin Anda nonaktifkan, pilih Non aktifkan standar.

Untuk menonaktifkan standar di Wilayah tambahan, ulangi langkah-langkah sebelumnya di setiap Wilayah tambahan.

Security Hub CSPM API

Untuk menonaktifkan standar secara terprogram dalam satu akun dan Wilayah, gunakan operasi. BatchDisableStandards Atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan batch-disable-standards perintah.

Dalam permintaan Anda, gunakan `StandardsSubscriptionArns` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari standar yang ingin Anda nonaktifkan. Jika Anda menggunakan AWS CLI, gunakan `standards-subscription-arns` parameter untuk menentukan ARN. Juga tentukan Wilayah tempat permintaan Anda berlaku. Misalnya, perintah berikut menonaktifkan standar F AWS oundational Security Best Practices (FSBP) untuk account (): *123456789012*

```
$ aws securityhub batch-disable-standards \
--standards-subscription-arns "arn:aws:securityhub:us-
east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0" \
--region us-east-1
```

Di *arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0* mana ARN standar FSBP untuk akun di Wilayah Timur AS (Virginia Utara), dan *us-east-1* merupakan Wilayah tempat menonaktifkannya.

Untuk mendapatkan ARN untuk standar, Anda dapat menggunakan GetEnabledStandards operasi. Operasi ini mengambil informasi tentang standar yang saat ini diaktifkan di akun Anda. Jika Anda menggunakan AWS CLI, Anda dapat menjalankan perintah get-enabled-standards untuk mengambil informasi ini.

Setelah Anda menonaktifkan standar, Security Hub CSPM mulai melakukan tugas untuk menonaktifkan standar di akun dan Wilayah yang ditentukan. Ini termasuk menonaktifkan semua kontrol yang berlaku untuk standar. Untuk memantau status tugas-tugas ini, Anda dapat memeriksa status standar untuk akun dan Wilayah.

Memahami kontrol keamanan di Security Hub CSPM

Dalam AWS Security Hub CSPM, kontrol keamanan, juga disebut sebagai kontrol, adalah perlindungan dalam standar keamanan yang membantu organisasi melindungi kerahasiaan,

integritas, dan ketersediaan informasinya. Di Security Hub CSPM, kontrol terkait dengan sumber daya tertentu AWS .

Saat Anda mengaktifkan kontrol dalam satu atau beberapa standar, Security Hub CSPM mulai menjalankan pemeriksaan keamanan di atasnya. Pemeriksaan keamanan menghasilkan temuan Security Hub CSPM. Saat Anda menonaktifkan kontrol, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan pada kontrol tersebut, dan temuan tidak lagi dihasilkan.

Anda dapat mengaktifkan atau menonaktifkan kontrol satu per satu untuk satu akun dan Wilayah AWS. Untuk menghemat waktu dan mengurangi penyimpangan konfigurasi di lingkungan multi-akun, sebaiknya gunakan konfigurasi pusat untuk mengaktifkan atau menonaktifkan kontrol. Dengan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan yang menentukan bagaimana kontrol harus dikonfigurasi di beberapa akun dan Wilayah. Untuk informasi selengkapnya tentang mengaktifkan dan menonaktifkan kontrol, lihatMengaktifkan kontrol di Security Hub CSPM.

Tampilan kontrol terkonsolidasi

Halaman Kontrol konsol CSPM Hub Keamanan menampilkan semua kontrol yang tersedia saat ini Wilayah AWS (Anda dapat melihat kontrol dalam konteks standar dengan mengunjungi halaman Standar keamanan dan memilih standar yang diaktifkan). Security Hub CSPM menetapkan kontrol ID kontrol keamanan yang konsisten, judul, dan deskripsi di seluruh standar. ID kontrol mencakup nomor yang relevan Layanan AWS dan unik (misalnya, CodeBuild.3).

Informasi berikut tersedia di halaman Kontrol konsol CSPM Hub Keamanan:

- Skor keamanan keseluruhan berdasarkan proporsi kontrol yang dilewati dibandingkan dengan jumlah total kontrol yang diaktifkan dengan data
- Rincian status kontrol di semua kontrol CSPM Security Hub yang didukung
- Jumlah total pemeriksaan keamanan yang lulus dan gagal.
- Jumlah pemeriksaan keamanan yang gagal untuk kontrol dengan tingkat keparahan yang bervariasi, dan tautan untuk melihat detail selengkapnya tentang pemeriksaan yang gagal tersebut.
- Daftar kontrol CSPM Security Hub, dengan filter untuk melihat subset kontrol tertentu.

Dari halaman Kontrol, Anda dapat memilih kontrol untuk melihat detailnya dan mengambil tindakan pada temuan yang dihasilkan oleh kontrol. Dari halaman ini, Anda juga dapat mengaktifkan atau menonaktifkan kontrol keamanan di Akun AWS dan Anda saat ini Wilayah AWS. Tindakan

pengaktifan dan penonaktifan dari halaman Kontrol berlaku di seluruh standar. Untuk informasi selengkapnya, lihat Mengaktifkan kontrol di Security Hub CSPM.

Untuk akun administrator, halaman Kontrol mencerminkan status kontrol di seluruh akun anggota. Jika pemeriksaan kontrol gagal di setidaknya satu akun anggota, status kontrol adalah Gagal. Jika Anda telah menetapkan Wilayah agregasi, halaman Kontrol mencerminkan status kontrol di semua Wilayah yang ditautkan. Jika pemeriksaan kontrol gagal di setidaknya satu Wilayah yang ditautkan, status kontrol adalah Gagal.

Tampilan kontrol konsolidasi menyebabkan perubahan pada bidang pencarian kontrol dalam Format Pen AWS emuan Keamanan (ASFF) yang dapat memengaruhi alur kerja. Untuk informasi selengkapnya, lihat Tampilan kontrol konsolidasi - Perubahan ASFF.

Ringkasan skor keamanan untuk kontrol

Halaman Kontrol menampilkan skor keamanan ringkasan dari 0-100 persen. Skor keamanan ringkasan dihitung berdasarkan proporsi kontrol yang dilewati dibandingkan dengan jumlah total kontrol yang diaktifkan dengan data lintas standar.

> **Note**
>
> Untuk melihat skor keamanan keseluruhan untuk kontrol, Anda harus menambahkan izin untuk memanggil **`BatchGetControlEvaluations`** peran IAM yang Anda gunakan untuk mengakses Security Hub CSPM. Izin ini tidak diperlukan untuk melihat skor keamanan untuk standar tertentu.

Saat Anda mengaktifkan Security Hub CSPM, Security Hub CSPM menghitung skor keamanan awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ring kasan atau halaman Standar Keamanan di konsol CSPM Hub Keamanan. Diperlukan waktu hingga 24 jam agar skor keamanan pertama kali dihasilkan di Wilayah China dan AWS GovCloud (US) Regions.

Selain skor keamanan keseluruhan, Security Hub CSPM menghitung skor keamanan standar untuk setiap standar yang diaktifkan dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ring kasan atau halaman Standar Keamanan. Untuk melihat daftar standar yang saat ini diaktifkan, gunakan operasi `GetEnabledStandards` API.

AWS Config harus diaktifkan dengan perekaman sumber daya agar skor muncul. Untuk informasi tentang cara Security Hub CSPM menghitung skor keamanan, lihat. Menghitung skor keamanan

Setelah pembuatan skor pertama kali, Security Hub CSPM memperbarui skor keamanan setiap 24 jam. Security Hub CSPM menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui.

Jika Anda telah menetapkan Wilayah agregasi, skor keamanan keseluruhan mencerminkan temuan kontrol di seluruh Wilayah yang ditautkan.

Referensi kontrol untuk Security Hub CSPM

Referensi kontrol ini menyediakan tabel kontrol CSPM AWS Security Hub yang tersedia dengan tautan ke informasi selengkapnya tentang setiap kontrol. Dalam tabel, kontrol dicantumkan dalam urutan abjad berdasarkan ID kontrol. Hanya kontrol yang digunakan aktif oleh Security Hub CSPM disertakan di sini. Kontrol yang dipensiunkan dikecualikan dari tabel.

Tabel ini memberikan informasi berikut untuk setiap kontrol:

- ID kontrol keamanan — ID ini berlaku di seluruh standar Layanan AWS dan menunjukkan sumber daya yang terkait dengan kontrol. Konsol CSPM Security Hub menampilkan ID kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan di akun Anda. Namun, temuan Security Hub CSPM mereferensikan ID kontrol keamanan hanya jika temuan kontrol konsolidasi diaktifkan di akun Anda. Jika temuan kontrol konsolidasi dinonaktifkan di akun Anda, beberapa ID kontrol bervariasi menurut standar dalam temuan kontrol Anda. Untuk pemetaan ID kontrol khusus standar ke ID kontrol keamanan, lihat. Bagaimana konsolidasi memengaruhi ID kontrol dan judul

  Jika Anda ingin mengatur otomatisasi untuk kontrol keamanan, sebaiknya filter berdasarkan ID kontrol daripada judul atau deskripsi. Sementara Security Hub CSPM kadang-kadang dapat memperbarui judul atau deskripsi kontrol, ID kontrol tetap sama.

  ID kontrol dapat melewati angka. Ini adalah placeholder untuk kontrol di masa mendatang.
- Judul kontrol keamanan - Judul ini berlaku di seluruh standar. Konsol Security Hub CSPM menampilkan judul kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan di akun Anda. Namun, temuan Security Hub CSPM mereferensikan judul kontrol keamanan hanya jika temuan kontrol konsolidasi diaktifkan di akun Anda. Jika temuan kontrol konsolidasi dimatikan di akun Anda, beberapa judul kontrol bervariasi menurut standar dalam temuan kontrol Anda. Untuk pemetaan ID kontrol khusus standar ke ID kontrol keamanan, lihat. Bagaimana konsolidasi memengaruhi ID kontrol dan judul
- Standar yang berlaku — Menunjukkan standar mana yang berlaku untuk kontrol. Pilih kontrol untuk meninjau persyaratan tertentu dari kerangka kerja kepatuhan pihak ketiga.

- Tingkat keparahan — Tingkat keparahan kontrol mengidentifikasi pentingnya dari sudut pandang keamanan. Untuk informasi tentang bagaimana Security Hub CSPM menentukan tingkat keparahan kontrol, lihat. Tingkat keparahan untuk temuan kontrol
- Mendukung parameter kustom - Menunjukkan apakah kontrol mendukung nilai kustom untuk satu atau lebih parameter. Pilih kontrol untuk meninjau detail parameter. Untuk informasi selengkapnya, lihat Memahami parameter kontrol di Security Hub CSPM.
- Jenis jadwal — Menunjukkan kapan kontrol dievaluasi. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Pilih kontrol untuk meninjau detail tambahan. Kontrol dicantumkan dalam urutan abjad berdasarkan ID kontrol keamanan.

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Account.1	Informasi kontak keamanan harus disediakan untuk Akun AWS	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Praktik Terbaik Keamanan Dasar v1.0.0, AWS NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
Account.2	Akun AWS harus menjadi bagian dari sebuah AWS Organizations organisasi	NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	periodik
ACM.1	Diimpor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST	SEDANG	⊙ Ya	Perubahan dipicu dan berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
		SP 800-171 Rev. 2, PCI DSS v4.0.1			
ACM.2	Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
ACM.3	Sertifikat ACM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Amplify.1	Aplikasi Amplify harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Amplify.2	Amplify cabang harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
APIGateway.1	API Gateway REST dan logging eksekusi WebSocket API harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	Perubahan dipicu
APIGateway.2	Tahap API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
APIGateway.3	Tahap API REST API Gateway API harus mengaktifkan AWS X-Ray pelacakan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
APIGateway.4	API Gateway harus dikaitkan dengan ACL Web WAF	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
APIGateway.5	Data cache API REST API Gateway harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
APIGateway.8	Rute API Gateway harus menentukan jenis otorisasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✓ Ya	periodik
APIGateway.9	Logging akses harus dikonfigurasi untuk API Gateway V2 Stages	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
APIGateway.10	Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
APIGateway.11	Nama domain API Gateway harus menggunakan kebijakan keamanan yang disarankan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
AppConfig.1	AWS AppConfig aplikasi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
AppConfig.2	AWS AppConfig profil konfigurasi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
AppConfig.3	AWS AppConfig lingkungan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
AppConfig.4	AWS AppConfig asosiasi ekstensi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
AppFlow.1	Ali AppFlow ran Amazon harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
AppRunner.1	Layanan App Runner harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
AppRunner.2	Konektor VPC App Runner harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AppSync.2	AWS AppSync harus mengaktifkan logging tingkat bidang	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v4.0.1	SEDANG	Ya	Perubahan dipicu
AppSync.4	AWS AppSync GraphQL API harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
AppSync.5	AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	Tidak	Perubahan dipicu
Athena.2	Katalog data Athena harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Athena.3	Kelompok kerja Athena harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Athena.4	Kelompok kerja Athena harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	Perubahan dipicu
AutoScaling.1	Grup Penskalaan Otomatis yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	RENDAH	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AutoScaling.2	Grup Penskalaan Otomatis Amazon EC2 harus mencakup beberapa Zona Ketersediaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Ya	Perubahan dipicu
AutoScaling.3	Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Instance Metadata Service Version 2 (IMDSv2)	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	Tidak	Perubahan dipicu
Autoscaling.5	Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	Tidak	Perubahan dipicu
AutoScaling.6	Grup Penskalaan Otomatis harus menggunakan beberapa jenis instans di beberapa Zona Ketersediaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
AutoScaling.9	Grup Penskalaan Otomatis EC2 harus menggunakan templat peluncuran EC2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Tidak	Perubahan dipicu
AutoScaling.10	Grup Penskalaan Otomatis EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Backup.1	AWS Backup titik pemulihan harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Tidak	Perubahan dipicu
Backup.2	AWS Backup titik pemulihan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Backup.3	AWS Backup brankas harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Backup.4	AWS Backup rencana laporan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Backup.5	AWS Backup rencana cadangan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Batch.1	Antrian pekerjaan batch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Batch.2	Kebijakan penjadwalan batch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Batch.3	Lingkungan komputasi batch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Batch.4	Properti sumber daya komputasi dalam lingkungan komputasi Batch terkelola harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Bedrock.1	Sumber data Amazon Bedrock harus dienkripsi dengan kunci yang dikelola AWS KMS pelanggan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	Perubahan dipicu
BedrockAgentCore.1	AgentCore Runtime dasar harus dikonfigurasi dengan mode jaringan VPC	AWS Praktik Terbaik Keamanan Dasar	TINGGI	Tidak	Perubahan dipicu
BedrockAgentCore.2	AgentCore Gateway Bedrock harus memerlukan otorisasi untuk permintaan masuk	AWS Praktik Terbaik Keamanan Dasar	TINGGI	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
BedrockAgentCore.3	Memori Bedrock AgentCore harus dienkripsi dengan kunci yang dikelola AWS KMS pelanggan	NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
BedrockAgentCore.4	Bedrock AgentCore Gateway harus dienkripsi dengan kunci yang dikelola AWS KMS pelanggan	NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
BedrockAgentCore.5	Peramban AgentCore kustom Bedrock seharusnya tidak menggunakan mode jaringan publik	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	Perubahan dipicu
BedrockAgentCore.6	Browser AgentCore khusus Bedrock harus mengaktifkan perekaman sesi	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
BedrockAgentCore.7	Penerjemah kode AgentCore kustom Bedrock harus menggunakan konfigurasi jaringan pribadi	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	Perubahan dipicu
CloudFormation.2	CloudFormation tumpukan harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudFormation.3	CloudFormation tumpukan harus mengaktifkan perlindungan penghentian	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFormation.4	CloudFormation tumpukan harus memiliki peran layanan terkait	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFront.1	CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
CloudFront.3	CloudFront distribusi harus memerlukan enkripsi dalam transit	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFront.4	CloudFront distribusi harus memiliki failover asal yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
CloudFront.5	CloudFront distribusi harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudFront.6	CloudFront distribusi harus mengaktifkan WAF	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFront.7	CloudFront distribusi harus menggunakan SSL/TLS sertifikat kustom	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	Perubahan dipicu
CloudFront.8	CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
CloudFront.9	CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFront.10	CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudFront.12	CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
CloudFront.13	CloudFront distribusi harus menggunakan kontrol akses asal	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFront.14	CloudFront Distribusi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
CloudFront.15	CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFront.16	CloudFront distribusi harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
CloudFront.17	CloudFront distribusi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail.1	CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, AWS Praktik Terbaik Keamanan Dasar, NIST AWS SP 800-53 Rev. 5	TINGGI	⊗ Tidak	periodik
CloudTrail.2	CloudTrail harus mengaktifkan enkripsi saat istirahat	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan CIS AWS v3.0.0, Benchmark Yayasan CIS AWS v1.2.0, Benchmark Yayasan CIS AWS v1.4.0 Praktik Terbaik Keamanan Dasar v1. AWS 0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
CloudTrail.3	Setidaknya satu CloudTrail jejak harus diaktifkan	NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	TINGGI	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail.4	CloudTrail Validasi file log harus diaktifkan	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan CIS AWS v3.0.0, Benchmark Yayasan CIS AWS v1.4.0, Benchmark Yayasan CIS AWS v1.2.0, Praktik Terbaik Keamanan Dasar v1.0.0, AWS NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1, PCI DSS v3.2.1	RENDAH	⊗ Tidak	periodik
CloudTrail.5	CloudTrail jalur harus diintegrasikan dengan Amazon CloudWatch Logs	Bench AWS mark Yayasan CIS v1.2.0, Benchmark AWS Yayasan CIS v1.4.0, Praktik Terbaik AWS Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
CloudTrail.6	Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	Benchmark AWS Yayasan CIS v1.2.0, Benchmark Yay AWS asan CIS v1.4.0, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu dan berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudTrail.7	Pastikan logging akses bucket S3 diaktifkan pada bucket CloudTrail S3	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan CIS AWS v3.0.0, Benchmark Yayasan CIS v1.2.0, Ben AWS chmark Yayasan CIS v1.4.0, Benchmark AWS Yayasan CIS v3.0.0, PCI DSS v4. AWS 0.1	RENDAH	⊗ Tidak	periodik
CloudTrail.9	CloudTrail jalur harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
CloudTrail.10	CloudTrail Penyimpanan data acara danau harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys	NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	periodik
CloudWatch.1	Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur AWS Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	RENDAH	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch.2	Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	Tolok AWS Ukur Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.3	Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA	Benchmark AWS Yayasan CIS v1.2.0	RENDAH	⊗ Tidak	periodik
CloudWatch.4	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.5	Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.6	Pastikan filter metrik log dan alarm ada untuk kegagalan Konsol Manajemen AWS otentikasi	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch.7	Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan CMK yang dibuat pelanggan	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.8	Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.9	Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.10	Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.11	Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CloudWatch.12	Pastikan filter metrik log dan alarm ada untuk perubahan pada gateway jaringan	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.13	Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.14	Pastikan filter metrik log dan alarm ada untuk perubahan VPC	Benchmark AWS Yayasan CIS v1.4.0, Tolok Ukur Yay AWS asan CIS v1.2.0, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	periodik
CloudWatch.15	CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	TINGGI	⊙ Ya	Perubahan dipicu
CloudWatch.16	CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu	NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	periodik
CloudWatch.17	CloudWatch tindakan alarm harus diaktifkan	NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
CodeArtifact.1	CodeArtifact repositori harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
CodeBuild.1	CodeBuild URL repositori sumber Bitbucket tidak boleh berisi kredenSIAL sensitif	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu
CodeBuild.2	CodeBuild variabel lingkungan proyek tidak boleh mengandung kredenSIAL teks yang jelas	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu
CodeBuild.3	CodeBuild Log S3 harus dienkripsi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	RENDAH	⊗ Tidak	Perubahan dipicu
CodeBuild.4	CodeBuild lingkungan proyek harus memiliki konfigurasi logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
CodeBuild.7	CodeBuild ekspor grup laporan harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
CodeGuruProfiler.1	CodeGuru Grup profil profiler harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
CodeGuruReviewer.1	CodeGuru Asosiasi repositori pengulas harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Cognito.1	Kumpulan pengguna Cognito harus memiliki perlindungan ancaman yang diaktifkan dengan mode penegakan fungsi penuh untuk otentikasi standar	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Ya	Perubahan dipicu
Cognito.2	Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	Perubahan dipicu
Cognito.3	Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Ya	Perubahan dipicu
Cognito.4	Kumpulan pengguna Cognito harus memiliki perlindungan ancaman yang diaktifkan dengan mode penegakan fungsi penuh untuk otentikasi khusus	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	Perubahan dipicu
Cognito.5	MFA harus diaktifkan untuk kumpulan pengguna Cognito	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Cognito.6	Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
Config.1	AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, AWS Praktik Terbaik Keamanan Dasar, NIST AWS SP 800-53 Rev. 5, PCI DSS v3.2.1	KRITIS	⊙ Ya	periodik
Connect.1	Hubungkan jenis objek Profil Pelanggan Pelanggan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Connect.2	Instans Connect Customer harus CloudWatch mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DataFirehose.1	Aliran pengirima n Firehose harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
DataSync.1	DataSync tugas harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
DataSync.2	DataSync tugas harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Detective.1	Grafik perilaku detektif harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
DMS.1	Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	⊗ Tidak	periodik
DMS.2	Sertifikat DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
DMS.3	Langganan acara DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
DMS.4	Instans replikasi DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DMS.5	Grup subnet replikasi DMS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
DMS.6	Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
DMS.7	Tugas replikasi DMS untuk database target harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
DMS.8	Tugas replikasi DMS untuk database sumber harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
DMS.9	Titik akhir DMS harus menggunakan SSL	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
DMS.10	Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
DMS.11	Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DMS.12	Titik akhir DMS untuk Redis OSS harus mengaktifkan TLS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
DMS.13	Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Zona Ketersediaan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
DocumentDB.1	Cluster Amazon DocumentDB harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
DocumentDB.2	Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊙ Ya	Perubahan dipicu
DocumentDB.3	Snapshot cluster manual Amazon DocumentDB tidak boleh bersifat publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu
DocumentDB.4	Cluster Amazon DocumentDB harus menerbitkan log audit ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DocumentDB.5	Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
DocumentDB.6	Cluster Amazon DocumentDB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
DynamoDB.1	Tabel DynamoDB harus secara otomatis menskalakan kapasitas dengan permintaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊘ Ya	periodik
DynamoDB.2	Tabel DynamoDB harus mengaktifkan pemulihan point-in-time	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
DynamoDB.3	Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
DynamoDB.4	Tabel DynamoDB harus ada dalam rencana cadangan	NIST SP 800-53 Rev. 5	SEDANG	⊘ Ya	periodik
DynamoDB.5	Tabel DynamoDB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊘ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
DynamoDB 6	Tabel DynamoDB harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
DynamoDB 7	Cluster DynamoDB Accelerator harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
EC2.1	Snapshot EBS tidak boleh dipulihkan secara publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	periodik
EC2.2	Grup keamanan default VPC seharusnya tidak mengizinkan lalu lintas masuk atau keluar	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS AWS v1.2.0, Praktik Terbaik Keamanan Dasar v1.0.0 AWS , PCI DSS v3.2.1, Benchmark Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5 AWS	TINGGI	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.3	Volume EBS terlampir harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
EC2.4	Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	periodik
EC2.6	Pencatatan aliran VPC harus diaktifkan di semua VPC	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan CIS AWS v3.0.0, Benchmark Yayasan CIS AWS v1.2.0, Praktik Terbaik Keamanan Dasar v1.0.0, AWS PCI DSS v3.2.1, Benchmark Yayasan CIS v1.4.0, NIST SP 800-53 Rev. 5, AWS NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.7	Enkripsi default EBS harus diaktifkan	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Praktik Terbaik Keamanan Dasar AWS v1.0.0, Benchmark Yayasan CIS v1.4.0, NIST SP 800- AWS 53 Rev. 5	SEDANG	⊗ Tidak	periodik
EC2.8	Instans EC2 harus menggunakan Instance Metadata Service Version 2 (IMDSv2)	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Praktik Terbaik Keamanan Das AWS ar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
EC2.9	Instans EC2 seharusnya tidak memiliki alamat IPv4 publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
EC2.10	Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.12	EIP EC2 yang tidak digunakan harus dihapus	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
EC2.13	Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 22	Bench AWS mark Yayasan CIS v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	TINGGI	⊗ Tidak	Perubahan dipicu dan berkala
EC2.14	Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 atau: :/0 ke port 3389	Benchmark AWS Yayasan CIS v1.2.0, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu dan berkala
EC2.15	Subnet EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	SEDANG	⊗ Tidak	Perubahan dipicu
EC2.16	Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1,	RENDAH	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.17	Instans EC2 tidak boleh menggunakan beberapa ENI	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
EC2.18	Grup keamanan hanya boleh mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	TINGGI	⊙ Ya	Perubahan dipicu
EC2.19	Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	KRITIS	⊗ Tidak	Perubahan dipicu dan berkala
EC2.20	Kedua terowongan AWS Site-to-Site VPN untuk koneksi VPN harus aktif	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.21	ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port 22 atau port 3389	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS AWS v1.4.0, Praktik Terbaik Keamanan Dasar, AWS NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
EC2.22	Grup keamanan EC2 yang tidak digunakan harus dihapus		SEDANG	⊗ Tidak	periodik
EC2.23	EC2 Transit Gateway seharusnya tidak secara otomatis menerima permintaan lampiran VPC	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
EC2.24	Jenis instance paravirtual EC2 tidak boleh digunakan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
EC2.25	Template peluncuran EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.28	Volume EBS harus dalam rencana cadangan	NIST SP 800-53 Rev. 5	RENDAH	Ya	periodik
EC2.33	Lampiran gateway transit EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.34	Tabel rute gateway transit EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.35	Antarmuka jaringan EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.36	Gateway pelanggan EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.37	Alamat IP Elastis EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.38	Instans EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.39	Gateway internet EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.40	Gateway EC2 NAT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.41	ACL jaringan EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.42	Tabel rute EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.43	Grup keamanan EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.44	Subnet EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.45	Volume EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.46	Amazon VPC harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.47	Layanan titik akhir Amazon VPC harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.48	Log aliran Amazon VPC harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.49	Koneksi peering Amazon VPC harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.50	Gateway VPN EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
EC2.51	Titik akhir VPN Klien EC2 harus mengaktifkan logging koneksi klien	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	RENDAH	✗ Tidak	Perubahan dipicu
EC2.52	Gateway transit EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
EC2.53	Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0.0/0 ke port administrasi server jarak jauh	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, PCI DSS v4.0.1	TINGGI	✗ Tidak	periodik
EC2.54	Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, PCI DSS v4.0.1	TINGGI	✗ Tidak	periodik
EC2.55	VPC harus dikonfigurasi dengan titik akhir antarmuka untuk API ECR	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	✓ Ya	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.56	VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Ya	periodik
EC2.57	VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Manajer Sistem	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Ya	periodik
EC2.58	VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Sistem	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Ya	periodik
EC2.60	VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Manajer Insiden Sistem Manajer Sistem	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Ya	periodik
EC2.170	Template peluncuran EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	RENDAH	Tidak	Perubahan dipicu
EC2.171	Koneksi EC2 VPN harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	SEDANG	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.172	Pengaturan Akses Publik Blok EC2 VPC harus memblokir lalu lintas gateway internet	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Ya	Perubahan dipicu
EC2.173	Permintaan EC2 Spot Fleet dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terpasang	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	Perubahan dipicu
EC2.174	Set opsi DHCP EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.175	Templat peluncuran EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.176	Daftar awalan EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.177	Sesi cermin lalu lintas EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
EC2.178	Filter cermin lalu lintas EC2 harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EC2.179	Target cermin lalu lintas EC2 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
EC2.180	Antarmuka jaringan EC2 harus mengaktifkan source/destination pemeriksaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	✗ Tidak	Perubahan dipicu
EC2.181	Template peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	✗ Tidak	Perubahan dipicu
EC2.182	Snapshot EBS seharusnya tidak dapat diakses publik	AWS Praktik Terbaik Keamanan Dasar	TINGGI	✗ Tidak	Perubahan dipicu
EC2.183	Koneksi EC2 VPN harus menggunakan protokol IKEv2	AWS Praktik Terbaik Keamanan Dasar	SEDANG	✗ Tidak	Perubahan dipicu
ECR.1	Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	✗ Tidak	periodik
ECR.2	Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECR.3	Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigu rasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ECR.4	Repositori publik ECR harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
ECR.5	Repositori ECR harus dienkripsi dengan pengelolaan pelanggan AWS KMS keys	NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	Perubahan dipicu
ECS.2	Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan secara otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
ECS.3	Definisi tugas ECS seharusnya tidak berbagi namespace proses host	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
ECS.4	Kontainer ECS harus berjalan sebagai non-hak istimewa	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.5	Wadah ECS harus dibatasi untuk akses read-only ke sistem file root	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
ECS.8	Rahasia tidak boleh diteruskan sebagai variabel lingkungan wadah	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
ECS.9	Definisi tugas ECS harus memiliki konfigurasi logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
ECS.10	Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
ECS.12	Cluster ECS harus menggunakan Container Insights	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ECS.13	Layanan ECS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
ECS.14	Cluster ECS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.15	Definisi tugas ECS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
ECS.16	Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	✗ Tidak	Perubahan dipicu
ECS.17	Definisi tugas ECS tidak boleh menggunakan mode jaringan host	NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu
ECS.18	Definisi Tugas ECS harus menggunakan enkripsi dalam transit untuk volume EFS	AWS Praktik Terbaik Keamanan Dasar	SEDANG	✗ Tidak	Perubahan dipicu
ECS.19	Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi terkelola	AWS Praktik Terbaik Keamanan Dasar	SEDANG	✗ Tidak	Perubahan dipicu
ECS.20	Definisi Tugas ECS harus mengonfigurasi pengguna non-root dalam definisi wadah Linux	AWS Praktik Terbaik Keamanan Dasar	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ECS.21	Definisi Tugas ECS harus mengonfigurasi pengguna non-admin istrator dalam definisi wadah Windows	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
EFS.1	Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Praktik Terbaik Keamanan Dasar v1.0.0, AWS NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
EFS.2	Volume Amazon EFS harus dalam rencana cadangan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
EFS.3	Titik akses EFS harus menerapkan direktori root	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
EFS.4	Titik akses EFS harus menegakkan identitas pengguna	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
EFS.5	Titik akses EFS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EFS.6	Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
EFS.7	Sistem file EFS harus mengaktifkan cadangan otomatis	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
EFS.8	Sistem file EFS harus dienkripsi saat diam	CIS Foun AWS dations Benchmark v5.0.0, Praktik Terbaik AWS Keamanan Dasar	SEDANG	✓ Ya	Perubahan dipicu
EKS.1	Titik akhir cluster EKS seharusnya tidak dapat diakses publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
EKS.2	Cluster EKS harus berjalan pada versi Kubernetes yang didukung	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
EKS.3	Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EKS.6	Cluster EKS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
EKS.7	Konfigurasi penyedia identitas EKS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
EKS.8	Cluster EKS harus mengaktifkan logging audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
EKS.9	Grup node EKS harus berjalan pada versi Kubernetes yang didukung	AWS Praktik Terbaik Keamanan Dasar	TINGGI	✗ Tidak	Perubahan dipicu
ElastiCache.1	ElastiCache Cluster (Redis OSS) harus mengaktifkan cadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	✓ Ya	periodik
ElastiCache.2	ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	✗ Tidak	periodik
ElastiCache.3	ElastiCache grup replikasi harus mengaktifkan failover otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ElastiCache.4	ElastiCache grup replikasi harus dienkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
ElastiCache.5	ElastiCache grup replikasi harus dienkripsi dalam transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
ElastiCache.6	ElastiCache Grup replikasi (Redis OSS) dari versi sebelumnya harus mengaktifkan Redis OSS AUTH	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
ElastiCache.7	ElastiCache cluster tidak boleh menggunakan grup subnet default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	periodik
ElasticBeanstalk.1	Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
ElasticBeanstalk.2	Pembaruan platform terkelola Elastic Beanstalk harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ElasticBeanstalk.3	Elastic Beanstalk harus mengalirkan log ke CloudWatch	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	✓ Ya	Perubahan dipicu
ELB.1	Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	periodik
ELB.2	Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	✗ Tidak	Perubahan dipicu
ELB.3	Pendengar Load Balancer Klasik harus dikonfigurasi dengan penghentian HTTPS atau TLS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
ELB.4	Application Load Balancer harus dikonfigurasi untuk melepaskan header http	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.5	Pencatatan aplikasi dan penyeimbang beban klasik harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ELB.6	Aplikasi, Gateway, dan Network Load Balancer harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ELB.7	Classic Load Balancer harus mengaktifkan pengeringan koneksi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
ELB.8	Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentuka n sebelumnya yang memiliki konfigurasi yang kuat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
ELB.9	Penyeimbang Beban Klasik harus mengaktifkan penyeimbangan beban lintas zona	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.10	Classic Load Balancer harus mencakup beberapa Zona Ketersediaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Ya	Perubahan dipicu
ELB.12	Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	Tidak	Perubahan dipicu
ELB.13	Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Ya	Perubahan dipicu
ELB.14	Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	Tidak	Perubahan dipicu
ELB.16	Penyeimbang Beban Aplikasi harus dikaitkan dengan ACL AWS web WAF	NIST SP 800-53 Rev. 5	SEDANG	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ELB.17	Aplikasi dan Penyeimbang Beban Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang disarankan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ELB.18	Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
ELB.21	Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
ELB.22	Kelompok target ELB harus menggunakan protokol transportasi terenkripsi	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
EMR.1	Node utama cluster Amazon EMR seharusnya tidak memiliki alamat IP publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EMR.2	Pengaturan akses publik blok Amazon EMR harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITIS	⊗ Tidak	periodik
EMR.3	Konfigurasi keamanan Amazon EMR harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
EMR.4	Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ES.1	Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
ES.2	Domain Elasticsearch seharusnya tidak dapat diakses publik	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	periodik
ES.3	Domain Elasticsearch harus mengenkripsi data yang dikirim antar node	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1,	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
ES.4	Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ES.5	Domain Elasticsearch harus mengaktifkan logging audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ES.6	Domain Elasticsearch harus memiliki setidaknya tiga node data	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ES.7	Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
ES.8	Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
ES.9	Domain Elasticsearch harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
EventBridge.2	EventBridge bus acara harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
EventBridge.3	EventBridge bus acara khusus harus memiliki kebijakan berbasis sumber daya yang dilampirkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	✗ Tidak	Perubahan dipicu
EventBridge.4	EventBridge titik akhir global harus mengaktifkan replikasi peristiwa	NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu
FraudDetector.1	Jenis entitas Amazon Fraud Detector harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
FraudDetector.2	Label Detektor Penipuan Amazon harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
FraudDetector.3	Hasil Amazon Fraud Detector harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
FraudDetector.4	Variabel Detektor Penipuan Amazon harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
FSx.1	FSX untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	periodik
FSx.2	Sistem file FSx untuk Lustre harus dikonfigurasi untuk menyalin tag ke cadangan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	periodik
FSx.3	FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
FSx.4	FSx untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊙ Ya	periodik
FSx.5	FSx untuk sistem file Server File Windows harus dikonfigurasi untuk penerapan Multi-AZ	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
Glue.1	AWS Glue pekerjaan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Glue.3	AWS Glue transformasi pembelajaran mesin harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
Glue.4	AWS Glue Pekerjaan Spark harus berjalan pada versi yang didukung AWS Glue	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
GlobalAccelerator.1	Akselerator Global Accelerator harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
GuardDuty.1	GuardDuty harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
GuardDuty.2	GuardDuty filter harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
GuardDuty.3	GuardDuty IPset harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
GuardDuty.4	GuardDuty detektor harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
GuardDuty.5	GuardDuty Pemantauan Log Audit EKS harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	periodik
GuardDuty.6	GuardDuty Perlindungan Lambda harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
GuardDuty.7	GuardDuty Pemantauan Runtime EKS harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
GuardDuty.8	GuardDuty Perlindungan Malware untuk EC2 harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	periodik
GuardDuty.9	GuardDuty Perlindungan RDS harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
GuardDuty.10	GuardDuty Perlindungan S3 harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
GuardDuty.11	GuardDuty Pemantauan Runtime harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	periodik
GuardDuty.12	GuardDuty ECS Runtime Monitoring harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
GuardDuty.13	GuardDuty EC2 Runtime Monitoring harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
IAM.1	Kebijakan IAM seharusnya tidak mengizinkan hak administratif penuh “*”	Bench AWS mark Yayasan CIS v1.2.0, Praktik AWS Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, Benchmark Yayasan CIS v1.4.0, NIST SP 800- AWS 53 Rev. 5, NIST SP 800-171 Rev. 2	TINGGI	⊗ Tidak	Perubahan dipicu
IAM.2	Pengguna IAM seharusnya tidak memiliki kebijakan IAM terlampir	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS AWS v1.2.0, Praktik Terbaik Keamanan Dasar v1.0.0, AWS PCI DSS v3.2.1, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.3	Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, AWS Praktik Terbaik Keamanan Dasar, NIST AWS SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
IAM.4	Kunci akses pengguna root IAM seharusnya tidak ada	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DS AWS S v3.2.1, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.5	MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, AWS Praktik Terbaik Keamanan Dasar, NIST AWS SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
IAM.6	Perangkat keras MFA harus diaktifkan untuk pengguna root	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan CIS AWS v3.0.0, Benchmark Yayasan CIS AWS v1.4.0, Benchmark Yayasan CIS AWS v1.2.0, Praktik Terbaik Keamanan Dasar, AWS NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.7	Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	Ya	periodik
IAM.8	Kredentif pengguna IAM yang tidak digunakan harus dihapus	Bench AWS mark Yayasan CIS v1.2.0, Prakti AWS k Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	SEDANG	Tidak	periodik
IAM.9	MFA harus diaktifkan untuk pengguna root	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan AWS CIS v3.0.0, Tolok Ukur Yayasan CIS AWS v1.4.0, Benchmark Yayasan CIS v1.2.0, NIS AWS T SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	Tidak	periodik
IAM.10	Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	NIST SP 800-171 Rev. 2, PCI DSS v3.2.1	SEDANG	Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.11	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf besar	Tolok AWS Ukur Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
IAM.12	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf kecil	Tolok AWS Ukur Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
IAM.13	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu simbol	Tolok AWS Ukur Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	periodik
IAM.14	Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu nomor	Tolok AWS Ukur Yayasan CIS v1.2.0, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.15	Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, NIST AWS SP 800-171 Rev. 2	SEDANG	⊗ Tidak	periodik
IAM.16	Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan AWS CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, NIS AWS T SP 800-171 Rev. 2, PCI DSS v4.0.1	RENDAH	⊗ Tidak	periodik
IAM.17	Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	Benchmark AWS Yayasan CIS v1.2.0, PCI DSS v4.0.1	RENDAH	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.18	Pastikan peran dukungan telah dibuat untuk mengelola insiden dengan AWS Dukungan	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan AWS CIS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0 AWS , Benchmark Yayasan CIS v1.2.0, NIS AWS T SP 800-171 Rev. 2, PCI DSS v4.0.1	RENDAH	⊗ Tidak	periodik
IAM.19	MFA harus diaktifkan untuk semua pengguna IAM	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
IAM.21	Kebijakan yang dikelola pelanggan IAM yang Anda buat tidak boleh mengizinkan tindakan wildcard untuk layanan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	Perubahan dipicu
IAM.22	KredenSIAL pengguna IAM yang tidak digunakan selama 45 hari harus dihapus	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, AWS NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IAM.23	Alat analisis IAM Access Analyzer harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IAM.24	Peran IAM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IAM.25	Pengguna IAM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IAM.26	SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS v AWS 3.0.0	SEDANG	✗ Tidak	periodik
IAM.27	Identitas IAM seharusnya tidak memiliki AWSCloudShellFullAccess kebijakan yang dilampirkan	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS v AWS 3.0.0	SEDANG	✗ Tidak	Perubahan dipicu
IAM.28	Penganalisis akses eksternal IAM Access Analyzer harus diaktifkan	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS v AWS 3.0.0	TINGGI	✗ Tidak	periodik
Inspector.1	Pemindaian Amazon Inspector EC2 harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	✗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Inspector.2	Pemindaian ECR Amazon Inspector harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
Inspector.3	Pemindaian kode Amazon Inspector Lambda harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
Inspector.4	Pemindaian standar Amazon Inspector Lambda harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
IoT.1	AWS IoT Device Defender profil keamanan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
IoT.2	AWS IoT Core Tindakan mitigasi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
IoT.3	AWS IoT Core dimensi harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
IoT.4	AWS IoT Core otorisasi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
IoT.5	AWS IoT Core alias peran harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IoT.6	AWS IoT Core Kebijakan harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoTSiteWise.1	AWS IoT SiteWise model asset harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoTSiteWise.2	AWS IoT SiteWise dasbor harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoTSiteWise.3	AWS IoT SiteWise gateway harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoTSiteWise.4	AWS IoT SiteWise portal harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoTSiteWise.5	AWS IoT SiteWise proyek harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoTTwinMaker.1	AWS Pekerjaan TwinMaker sinkronisasi IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
IoTTwinMaker.2	AWS TwinMaker Ruang kerja IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
IoTTwinMaker.3	AWS A TwinMaker degan IoT harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IoTTwinMaker.4	AWS Enti TwinMaker tas IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IoTWireless.1	AWS Grup multicast Nirkabel IoT harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IoTWireless.2	AWS Profil layanan IoT Wireless harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IoTWireless.3	AWS Tugas FUOTA Nirkabel IoT harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IVS.1	Pasangan kunci pemutaran IVS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IVS.2	Konfigurasi perekaman IVS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
IVS.3	Saluran IVS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
Keyspaces.1	Ruang kunci Amazon Keyspaces harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Kinesis.1	Aliran Kinesis harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Kinesis.2	Streaming kinesis harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Kinesis.3	Streaming kinesis harus memiliki periode retensi data yang memadai	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊙ Ya	Perubahan dipicu
KMS.1	Kebijakan yang dikelola pelanggan IAM seharusnya tidak mengizinkan tindakan dekripsi pada semua kunci KMS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
KMS.2	Prinsipal IAM seharusnya tidak memiliki kebijakan sebaris IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
KMS.3	AWS KMS keys tidak boleh dihapus secara tidak sengaja	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
KMS.4	AWS KMS key rotasi harus diaktifkan	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, AWS Tolok Ukur Yayasan CIS AWS v1.2.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
KMS.5	Kunci KMS seharusnya tidak dapat diakses publik	AWS Praktik Terbaik Keamanan Dasar	KRITIS	⊗ Tidak	Perubahan dipicu
Lambda.1	Kebijakan fungsi lambda harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu
Lambda.2	Fungsi lambda harus menggunakan runtime yang didukung	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
Lambda.3	Fungsi lambda harus dalam VPC	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
Lambda.5	Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Lambda.6	Fungsi lambda harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
Lambda.7	Fungsi lambda harus mengaktifkan pelac AWS X-Ray akan aktif	NIST SP 800-53 Rev. 5	RENDAH	✗ Tidak	Perubahan dipicu
Macie.1	Amazon Macie harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	periodik
Macie.2	Penemuan data sensitif otomatis Macie harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	✗ Tidak	periodik
MSK.1	Cluster MSK harus dienkripsi dalam transit di antara node broker	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
MSK.2	Cluster MSK harus memiliki pemantaua n yang ditingkatkan dikonfigurasi	NIST SP 800-53 Rev. 5	RENDAH	✗ Tidak	Perubahan dipicu
MSK.3	Konektor MSK Connect harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
MSK.4	Cluster MSK harus memiliki akses publik yang dinonaktifkan	AWS Praktik Terbaik Keamanan Dasar	KRITIS	⊗ Tidak	Perubahan dipicu
MSK.5	Konektor MSK harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
MSK.6	Cluster MSK harus menonaktifkan akses yang tidak diautenti kasi	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
MQ.2	Broker ActiveMQ harus melakukan streaming log audit ke CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
MQ.4	Broker Amazon MQ harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
MQ.5	Broker ActiveMQ harus menggunakan mode penyebaran active/standby	NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
MQ.6	Broker RabbitMQ harus menggunakan mode penyebaran cluster	NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Neptune.1	Cluster DB Neptune harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Neptune.2	Cluster Neptune DB harus menerbitkan log audit ke CloudWatch Log	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
Neptune.3	Snapshot cluster Neptune DB tidak boleh publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu
Neptune.4	Cluster Neptune DB harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
Neptune.5	Cluster Neptune DB harus mengaktifkan cadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✓ Ya	Perubahan dipicu
Neptune.6	Snapshot cluster Neptune DB harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Neptune.7	Cluster Neptune DB harus mengaktifkan otentikasi database IAM	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Neptune.8	Cluster Neptune DB harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
Neptune.9	Cluster DB Neptune harus digunakan di beberapa Zona Ketersediaan	NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
NetworkFirewall.1	Firewall Network Firewall harus digunakan di beberapa Availability Zone	NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
NetworkFirewall.2	Pencatatan Firewall Jaringan harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	periodik
NetworkFirewall.3	Kebijakan Firewall Jaringan harus memiliki setidaknya satu grup aturan yang terkait	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	Perubahan dipicu
NetworkFirewall.4	Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket lengkap	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
NetworkFirewall.5	Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket terfragmentasi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	Perubahan dipicu
NetworkFirewall.6	Grup aturan firewall jaringan stateless tidak boleh kosong	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	Perubahan dipicu
NetworkFirewall.7	Firewall Network Firewall harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
NetworkFirewall.8	Kebijakan firewall Network Firewall harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
NetworkFirewall.9	Firewall Network Firewall harus mengaktifkan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
NetworkFirewall.10	Firewall Network Firewall harus mengaktifkan perlindungan perubahan subnet	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Opensearch.1	OpenSearch domain harus mengaktifkan enkripsi saat istirahat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Opensearch.2	OpenSearch domain seharusnya tidak dapat diakses publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	Perubahan dipicu
Opensearch.3	OpenSearch domain harus mengenkripsi data yang dikirim antar node	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Opensearch.4	OpenSearch pencatatan kesalahan domain ke CloudWatch Log harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Opensearch.5	OpenSearch domain harus mengaktifkan logging audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
Opensearch.6	OpenSearch domain harus memiliki setidaknya tiga node data	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Opensearch.7	OpenSearch domain harus mengaktifkan kontrol akses halus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
Opensearch.8	Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Opensearch.9	OpenSearch domain harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Opensearch.10	OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
Opensearch.11	OpenSearch domain harus memiliki setidaknya tiga node utama khusus	NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	periodik
PCA.1	AWS Private CA otoritas sertifikat root harus dinonaktifkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	periodik
PCA.2	AWS Otoritas sertifikat CA pribadi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.1	Snapshot RDS harus bersifat pribadi	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	Perubahan dipicu
RDS.2	Instans DB RDS harus melarang akses publik, sebagaima na ditentukan oleh konfigurasi PubliclyA ccessible	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Praktik Terbaik Keamanan Das AWS ar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu
RDS.3	Instans DB RDS harus mengaktifkan enkripsi saat istirahat	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Praktik Terbaik Keamanan Dasar v1.0.0 AWS , NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
RDS.4	Snapshot cluster RDS dan snapshot database harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.5	Instans RDS DB harus dikonfigurasi dengan beberapa Zona Ketersediaan	Benchmark AWS Yayasan CIS v5.0.0, Praktik Terbaik AWS Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
RDS.6	Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans DB RDS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊙ Ya	Perubahan dipicu
RDS.7	Cluster RDS harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
RDS.8	Instans DB RDS harus mengaktif kan perlindungan penghapusan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.9	Instans DB RDS harus menerbitkan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
RDS.10	Otentikasi IAM harus dikonfigurasi untuk instans RDS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.11	Instans RDS harus mengaktifkan pencadangan otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Ya	Perubahan dipicu
RDS.12	Otentikasi IAM harus dikonfigurasi untuk cluster RDS	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Tidak	Perubahan dipicu
RDS.13	Upgrade versi minor otomatis RDS harus diaktifkan	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Praktik Terbaik Keamanan Das AWS ar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	Tidak	Perubahan dipicu
RDS.14	Cluster Amazon Aurora harus mengaktifkan backtracking	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Ya	Perubahan dipicu
RDS.15	Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan	Benchmark AWS Yayasan CIS v5.0.0, Praktik Terbaik AWS Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.16	Cluster Aurora DB harus dikonfigurasi untuk menyalin tag ke snapshot DB	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.17	Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.19	Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa cluster kritis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.20	Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.21	Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.22	Langganan notifikasi peristiwa RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.23	Instans RDS tidak boleh menggunakan port default mesin database	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.24	Cluster Database RDS harus menggunakan nama pengguna administrator khusus	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
RDS.25	Instans database RDS harus menggunakan nama pengguna administrator khusus	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
RDS.26	Instans DB RDS harus dilindungi oleh rencana cadangan	NIST SP 800-53 Rev. 5	SEDANG	✓ Ya	periodik
RDS.27	Cluster DB RDS harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.28	Cluster RDS DB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
RDS.29	Snapshot cluster RDS DB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
RDS.30	Instans DB RDS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
RDS.31	Grup keamanan RDS DB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
RDS.32	Snapshot DB RDS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
RDS.33	Grup subnet RDS DB harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
RDS.34	Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu
RDS.35	Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.36	Instans RDS untuk PostgreSQL DB harus menerbitkan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	SEDANG	Ya	Perubahan dipicu
RDS.37	Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	SEDANG	Tidak	Perubahan dipicu
RDS.38	Instans RDS untuk PostgreSQL DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	periodik
RDS.39	RDS untuk instans MySQL DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	periodik
RDS.40	RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Ya	Perubahan dipicu
RDS.41	RDS untuk instans SQL Server DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	periodik
RDS.42	RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Ya	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.43	Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
RDS.44	RDS untuk instans MariaDB DB harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
RDS.45	Cluster Aurora MySQL DB harus mengaktifkan logging audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
RDS.46	Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	periodik
RDS.47	RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB	AWS Praktik Terbaik Keamanan Dasar	RENDAH	⊗ Tidak	Perubahan dipicu
RDS.48	RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB	AWS Praktik Terbaik Keamanan Dasar	RENDAH	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RDS.50	Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Ya	Perubahan dipicu
RDS.51	Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	Perubahan dipicu
Redshift.1	Cluster Amazon Redshift harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu
Redshift.2	Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
Redshift.3	Cluster Amazon Redshift harus mengaktifkan snapshot otomatis	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	Perubahan dipicu
Redshift.4	Cluster Amazon Redshift harus mengaktifkan pencatatan audit	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Redshift.6	Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Redshift.7	Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Redshift.8	Amazon Redshift cluster tidak boleh menggunakan nama pengguna Admin default	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Redshift.10	Cluster pergeseran merah harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
Redshift.11	Cluster pergeseran merah harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Redshift.12	Pemberitahuan berlangganan acara Redshift harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
Redshift.13	Snapshot cluster pergeseran merah harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Redshift.14	Grup subnet cluster pergeseran merah harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
Redshift.15	Grup keamanan Redshift harus mengizinkan masuknya pada port cluster hanya dari sumber terbatas	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	✗ Tidak	periodik
Redshift.16	Grup subnet cluster Redshift harus memiliki subnet dari beberapa Zona Ketersediaan	NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu
Redshift.17	Grup parameter cluster pergeseran merah harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
Redshift.18	Cluster Redshift harus mengaktifkan pener Multi-AZ apan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	✗ Tidak	Perubahan dipicu
RedshiftServerless.1	Kelompok kerja Amazon Redshift Serverless harus menggunakan perutean VPC yang ditingkatkan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	✗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
RedshiftServerless.2	Koneksi ke kelompok kerja Redshift Serverless harus diperlukan untuk menggunakan SSL	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
RedshiftServerless.3	Kelompok kerja Redshift Serverless harus melarang akses publik	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	periodik
RedshiftServerless.4	Ruang nama Redshift Serverless harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys	NIST SP 800-53 Rev. 5	SEDANG	⊙ Ya	periodik
RedshiftServerless.5	Redshift Serverless namespace tidak boleh menggunakan nama pengguna admin default	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
RedshiftServerless.6	Redshift Serverless namespace harus mengekspor log ke Log CloudWatch	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
Route53.1	Pemeriksaan kesehatan rute 53 harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Route53.2	Zona host publik Route 53 harus mencatat kueri DNS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
S3.1	Bucket tujuan umum S3 harus mengaktif kan pengaturan akses publik blok	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Praktik Terbaik Keamanan Dasar, AWS NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
S3.2	Bucket tujuan umum S3 harus memblokir akses baca publik	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	Perubahan dipicu dan berkala
S3.3	Bucket tujuan umum S3 harus memblokir akses tulis publik	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	Perubahan dipicu dan berkala

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.5	Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan CIS AWS v3.0.0, Benchmark Yayasan CIS AWS v1.4.0, Praktik Terbaik Keamanan Dasar, AWS NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
S3.6	Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	TINGGI	⊗ Tidak	Perubahan dipicu
S3.7	Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah	PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.8	Bucket tujuan umum S3 harus memblokir akses publik	Benchmark AWS Yayasan CIS v5.0.0, Benchmark Yayasan AWS CIS v3.0.0, Benchmark Yayasan CIS v1.4.0 AWS , Praktik Terbaik Keamanan Dasar, AWS NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
S3.9	Bucket tujuan umum S3 harus mengaktif kan logging akses server	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
S3.10	Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
S3.11	Bucket tujuan umum S3 harus mengaktif kan notifikasi acara	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	✓ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.12	ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
S3.13	Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	RENDAH	⊙ Ya	Perubahan dipicu
S3.14	Bucket tujuan umum S3 harus mengaktif kan pembuatan versi	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	RENDAH	⊗ Tidak	Perubahan dipicu
S3.15	Bucket tujuan umum S3 harus mengaktif kan Object Lock	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊙ Ya	Perubahan dipicu
S3.17	Bucket tujuan umum S3 harus dienkrips i saat diam dengan AWS KMS keys	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
S3.19	Titik akses S3 harus mengaktifkan pengaturan akses publik blok	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	KRITIS	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
S3.20	Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, Tolok Ukur Yayasan CIS v1.4.0, AWS NIST SP 800-53 Rev. 5	RENDAH	⊗ Tidak	Perubahan dipicu
S3.22	Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
S3.23	Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek	Benchmark AWS Yayasan CIS v5.0.0, Tolok Ukur Yayasan CIS AWS v3.0.0, PCI DSS v4.0.1	SEDANG	⊗ Tidak	periodik
S3.24	S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok	AWS Praktik Terbaik Keamanan Dasar, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
S3.25	Bucket direktori S3 harus memiliki konfigurasi siklus hidup	AWS Praktik Terbaik Keamanan Dasar	RENDAH	✓ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SageMaker.1	Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	TINGGI	⊗ Tidak	periodik
SageMaker.2	SageMaker instans notebook harus diluncurkan dalam VPC khusus	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
SageMaker.3	Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	TINGGI	⊗ Tidak	Perubahan dipicu
SageMaker.4	SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	periodik
SageMaker.5	SageMaker model harus mengaktifkan isolasi jaringan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.6	SageMaker konfigurasi gambar aplikasi harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
SageMaker.7	SageMaker gambar harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SageMaker.8	SageMaker Instans notebook harus berjalan pada platform yang didukung	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	periodik
SageMaker.9	SageMaker definisi pekerjaan kualitas data harus mengaktifkan enkripsi lalu lintas antar kontainer	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.10	SageMaker definisi pekerjaan penjelasan model harus mengaktifkan enkripsi lalu lintas antar kontainer	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.11	SageMaker definisi pekerjaan kualitas data harus mengaktifkan isolasi jaringan	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.12	SageMaker definisi pekerjaan bias model harus mengaktifkan isolasi jaringan	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.13	SageMaker definisi pekerjaan kualitas model harus mengaktifkan enkripsi lalu lintas antar kontainer	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SageMaker.14	SageMaker jadwal pemantauan harus mengaktifkan isolasi jaringan	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.15	SageMaker definisi pekerjaan bias model harus mengaktifkan enkripsi lalu lintas antar kontainer	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.16	SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.17	SageMaker grup fitur toko offline harus dienkripsi dengan AWS KMS kunci	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.18	SageMaker grup fitur toko online dengan penyimpanan standar harus dienkripsi dengan AWS KMS kunci	NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.19	SageMaker model harus menggunakan registri pribadi di VPC untuk pipeline inferensi multi-kontainer	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SageMaker.20	SageMaker definisi pekerjaan penjelasan model harus mengaktifkan isolasi jaringan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	Perubahan dipicu
SageMaker.21	SageMaker Instans notebook harus dienkripsi dengan AWS KMS kunci yang dikelola pelanggan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.22	SageMaker jadwal pemantauan harus mengaktifkan enkripsi lalu lintas antar kontainer	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.23	SageMaker eksperimen inferensi harus memiliki volume penyimpanan instance yang dienkripsi dengan kunci yang dikelola AWS KMS pelanggan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SageMaker.24	SageMaker eksperimen inferensi harus memiliki penyimpanan data yang dienkripsi dengan kunci yang dikelola AWS KMS pelanggan	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
SageMaker.25	SageMaker definisi pekerjaan kualitas model harus mengaktifkan isolasi jaringan	AWS Praktik Terbaik Keamanan Dasar	TINGGI	⊗ Tidak	Perubahan dipicu
SecretsManager.1	Rahasia Manajer Rahasia harus mengaktifkan rotasi otomatis	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✓ Ya	Perubahan dipicu
SecretsManager.2	Rahasia Manajer Rahasia yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	⊗ Tidak	Perubahan dipicu
SecretsManager.3	Hapus rahasia Manajer Rahasia yang tidak digunakan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	✓ Ya	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SecretsManager.4	Rahasia Manajer Rahasia harus dirotasi dalam jumlah hari tertentu	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	Ya	periodik
SecretsManager.5	Rahasia Manajer Rahasia harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
ServiceCatalog.1	Portofolio Katalog Layanan harus dibagikan dalam AWS organisasi saja	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Tidak	periodik
SES.1	Daftar kontak SES harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
SES.2	Set konfigurasi SES harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
SES.3	Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email	AWS Praktik Terbaik Keamanan Dasar	SEDANG	Tidak	Perubahan dipicu
SNS.1	Topik SNS harus dienkripsi saat istirahat menggunakan AWS KMS	NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SNS.3	Topik SNS harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
SNS.4	Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik	AWS Praktik Terbaik Keamanan Dasar	KRITIS	✗ Tidak	Perubahan dipicu
SQS.1	Antrian Amazon SQS harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu
SQS.2	Antrian SQS harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
SQS.3	Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik	AWS Praktik Terbaik Keamanan Dasar	KRITIS	✗ Tidak	Perubahan dipicu
SSM.1	Instans EC2 harus dikelola oleh AWS Systems Manager	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
SSM.2	Instans EC2 yang dikelola oleh Manajer Sistem harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2, PCI DSS v3.2.1, PCI DSS v4.0.1	TINGGI	⊗ Tidak	Perubahan dipicu
SSM.3	Instans EC2 yang dikelola oleh Manajer Sistem harus memiliki status kepatuhan asosiasi COMPLIANT	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, PCI DSS v3.2.1, PCI DSS v4.0.1	RENDAH	⊗ Tidak	Perubahan dipicu
SSM.4	Dokumen SSM tidak boleh bersifat publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	KRITIS	⊗ Tidak	periodik
SSM.5	Dokumen SSM harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	⊙ Ya	Perubahan dipicu
SSM.6	Otomasi SSM harus mengaktifkan CloudWatch logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0	SEDANG	⊗ Tidak	periodik
SSM.7	Dokumen SSM harus mengaktifkan pengaturan pemblokiran berbagi publik	AWS Praktik Terbaik Keamanan Dasar v1.0.0	KRITIS	⊗ Tidak	periodik

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
StepFunctions.1	Fungsi Langkah Mesin status harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar v1.0.0, PCI DSS v4.0.1	SEDANG	Ya	Perubahan dipicu
StepFunctions.2	Aktivitas Fungsi Langkah harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Transfer.1	Alur kerja Transfer Family harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Transfer.2	Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	Tidak	periodik
Transfer.3	Konektor Transfer Family harus mengaktifkan logging	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5	SEDANG	Tidak	Perubahan dipicu
Transfer.4	Perjanjian Keluarga Transfer harus ditandai	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu
Transfer.5	Sertifikat Transfer Keluarga harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	Ya	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
Transfer.6	Konektor Transfer Family harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
Transfer.7	Profil Transfer Keluarga harus diberi tag	AWS Standar Penandaan Sumber Daya	RENDAH	✓ Ya	Perubahan dipicu
WAF.1	AWS Pencatatan ACL Web Global WAF Classic harus diaktifkan	AWS Praktik Terbaik Keamanan Dasar, NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	SEDANG	✗ Tidak	periodik
WAF.2	AWS Aturan WAF Classic Regional harus memiliki setidaknya satu syarat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu
WAF.3	AWS Kelompok aturan Regional Klasik WAF harus memiliki setidaknya satu aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu
WAF.4	AWS ACL web Regional WAF Classic harus memiliki setidaknya satu aturan atau grup aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	✗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
WAF.6	AWS Aturan global WAF Classic harus memiliki setidaknya satu syarat	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
WAF.7	AWS Kelompok aturan global WAF Classic harus memiliki setidaknya satu aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
WAF.8	AWS ACL web global WAF Classic harus memiliki setidaknya satu aturan atau grup aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
WAF.10	AWS ACL web WAF harus memiliki setidaknya satu aturan atau grup aturan	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5	SEDANG	⊗ Tidak	Perubahan dipicu
WAF.11	AWS Pencatatan ACL web WAF harus diaktifkan	NIST SP 800-53 Rev. 5, PCI DSS v4.0.1	RENDAH	⊗ Tidak	periodik
WAF.12	AWS Aturan WAF harus mengaktifkan CloudWatch metrik	AWS Praktik Terbaik Keamanan Dasar v1.0.0, NIST SP 800-53 Rev. 5, NIST SP 800-171 Rev. 2	SEDANG	⊗ Tidak	Perubahan dipicu

ID kontrol keamanan	Judul kontrol keamanan	Standar yang berlaku	Kepelikan	Mendukung parameter kustom	Jenis jadwal
WorkSpaces.1	WorkSpaces volume pengguna harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu
WorkSpaces.2	WorkSpaces volume root harus dienkripsi saat diam	AWS Praktik Terbaik Keamanan Dasar	SEDANG	⊗ Tidak	Perubahan dipicu

Log perubahan untuk kontrol CSPM Security Hub

Log perubahan berikut melacak perubahan material pada kontrol CSPM AWS Security Hub yang ada, yang dapat mengakibatkan perubahan pada status keseluruhan kontrol dan status kepatuhan temuannya. Untuk informasi tentang cara Security Hub CSPM mengevaluasi status kontrol, lihat. Mengevaluasi status kepatuhan dan status kontrol Perubahan dapat memakan waktu beberapa hari setelah entri di log ini untuk mempengaruhi semua Wilayah AWS di mana kontrol tersedia.

Log ini melacak perubahan yang terjadi sejak April 2023. Pilih kontrol untuk meninjau detail tambahan tentangnya. Perubahan judul dicatat dalam deskripsi rinci kontrol selama 90 hari.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
September 11, 2026	[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis	Kontrol ini memeriksa apakah peningkatan versi minor otomatis diaktifkan untuk cluster Amazon RDS DB. Security Hub CSPM memperluas kontrol untuk mengevaluasi cluster Aurora DB, yang sebelumnya tidak

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
		mengembalikan temuan.
September 11, 2026	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS	Security Hub CSPM memperbarui judul dan deskripsi kontrol ini untuk merujuk ke TLS alih-alih SSL karena SSL tidak digunakan lagi.
Agustus 27, 2026	[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible	Kontrol ini memeriksa apakah instans Amazon RDS melarang akses publik. Karena Neptune DB sekarang mendukung titik akhir publik, kontrol ini mengevaluasi dan menghasilkan temuan yang dapat ditindaklanjuti untuk instans Neptune DB. Security Hub CSPM memperbarui deskripsi kontrol untuk mencerminkan perubahan ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Agustus 12, 2026	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon EKS berjalan pada versi Kubernetes yang didukung. Security Hub CSPM mengubah nilai parameter untuk kontrol ini dari `1.33` ke. `1.34` Dukungan standar untuk Kubernetes versi 1.33 di Amazon EKS berakhir pada 29 Juli 2026.
Agustus 12, 2026	[EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah grup simpul Amazon EKS berjalan pada versi Kubernetes yang didukung. Security Hub CSPM mengubah nilai parameter untuk kontrol ini dari `1.33` ke. `1.34` Dukungan standar untuk Kubernetes versi 1.33 di Amazon EKS berakhir pada 29 Juli 2026.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
3 Agu 2026	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `java17.al2023`, `java11.al2023`, `java8.al2023` sebagai nilai parameter seperti yang AWS Lambda telah menambahkan dukungan untuk runtime ini.
3 Agu 2026	[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan	Security Hub CSPM telah menghapus kontrol ini dari standar F AWS oundational Security Best Practices (FSBP).

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juli 31, 2026	[SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung	Security Hub CSPM mengubah nilai parameter untuk kontrol ini dari `notebook-al2-v3` ke. `notebook-al2023-v1` SageMaker AI memigrasikan platform instance notebook dari Amazon Linux 2 ke AL2023.
Juli 13, 2026	[EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2	Security Hub CSPM mengubah aturan dukungan untuk kontrol ini dari service-vpc-endpoint-enabled menjadi vpc-endpoint-enabled. Aturan yang diperbarui mengenali FIPS-varian nama layanan titik akhir sebagai sesuai dan menghasilkan tem `PASSED` uan untuk VPC yang menggunakan titik akhir FIPS.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juni 29, 2026	[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan	Security Hub CSPM telah menambahk an kontrol ini ke standar yang berlaku berikut - standar NIST SP 800-53 Rev. 5, standar NIST SP 800-171 Revisi 2, dan standar PCI DSS v4.0.1. https:// docs.aws.amazon.co m/securityhub/latest/ userguide/pci-standa rd.html Pada 30 Juli 2026, kontrol ini akan dihapus dari standar Praktik Terbaik AWS Keamanan Dasar (FSBP).

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
5 Juni 2026	[EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi	Security Hub CSPM memberikan pemberitahuan bahwa kontrol ini akan dihentikan dan dihapus dari semua standar CSPM Hub Keamanan yang berlaku setelah 10 Agustus 2026. Dimulai dengan Kubernetes versi 1.28, cluster Amazon EKS memiliki rahasia Kubernetes yang dilindungi dengan enkripsi amplop secara default.
5 Juni 2026	[IoTEvents.1] IoTEvents.1	Security Hub CSPM memberikan pemberitahuan bahwa kontrol ini akan dihentikan dan dihapus dari semua standar CSPM Hub Keamanan yang berlaku setelah 7 Juli 2026. AWS mengumumkan akhir dukungan untuk layanan AWS Acara IoT efektif 20 Mei 2026.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
5 Juni 2026	[IoTEvents.2] IoTEvents.2	Security Hub CSPM memberikan pemberitahuan bahwa kontrol ini akan dihentikan dan dihapus dari semua standar CSPM Hub Keamanan yang berlaku setelah 7 Juli 2026. AWS mengumumkan akhir dukungan untuk layanan AWS Acara IoT efektif 20 Mei 2026.
5 Juni 2026	[IoTEvents.3] IoTEvents.3	Security Hub CSPM memberikan pemberitahuan bahwa kontrol ini akan dihentikan dan dihapus dari semua standar CSPM Hub Keamanan yang berlaku setelah 7 Juli 2026. AWS mengumumkan akhir dukungan untuk layanan AWS Acara IoT efektif 20 Mei 2026.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
5 Juni 2026	[ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar yang berlaku. Sebelumnya, kontrol memeriksa apakah definisi tugas Amazon ECS aktif yang menggunakan mode jaringan host juga memiliki definisi `privileged` atau `user` kontainer.
5 Juni 2026	[RDS.18] Instans RDS harus digunakan dalam VPC	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar yang berlaku. Sejak EC2-Class ic jaringan Amazon dihentikan, instans Amazon Relationa l Database Service (Amazon RDS) tidak dapat lagi digunakan di luar VPC. Sebelumnya, kontrol memeriksa apakah instance Amazon RDS digunakan pada. EC2-VPC

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
4 Mei 2026	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `ruby4.0` sebagai parameter dan tidak lagi menyertakan `nodejs20.x` karena AWS Lambda telah menghentikan runtime ini.
April 27, 2026	[EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu	Security Hub CSPM mengubah aturan dukungan untuk kontrol ini dari ec2-stoped-instance menjadi aturan CSPM Hub Keamanan kustom, ec2-stoped-instance-days-check untuk menyederhanakan logika evaluasi.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
7 April 2026	[EC2.1] Snapshot Amazon EBS tidak boleh dikonfigurasi agar dapat dipulihkan secara publik	Security Hub CSPM mengubah judul dan deskripsi kontrol ini. Judul dan deskripsi baru lebih akurat mencerminkan bahwa kontrol memeriksa apakah snapshot Amazon EBS dikonfigurasi agar dapat dipulihkan secara publik. Sebelumnya, judul kontrol ini adalah: Snapshot Amazon EBS tidak boleh dipulihkan secara publik.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
7 April 2026	[EC2.182] Blokir pengaturan akses publik harus diaktifkan untuk snapshot Amazon EBS	Security Hub CSPM mengubah judul dan deskripsi kontrol ini. Judul dan deskripsi baru lebih akurat mencerminkan bahwa kontrol memeriksa apakah akses publik blok tingkat akun diaktifkan untuk snapshot Amazon EBS. Sebelumnya, judul kontrol ini adalah: Amazon EBS Snapshots tidak boleh diakses publik.
6 April 2026	[ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan	Security Hub CSPM memperbarui nilai parameter untuk kontrol ini untuk mencerminkan kebijakan keamanan yang direkomendasikan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
3 April 2026	[Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat	Security Hub CSPM memperluas jangkauan nilai yang didukung untuk `temporaryPasswordValidity` parameter kontrol ini. Anda sekarang dapat menentukan nilai mulai dari 1-365 hari. Sebelumnya, kisarannya adalah 7-365 hari.
3 April 2026	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon EKS berjalan pada versi Kubernetes yang didukung. Security Hub CSPM mengubah nilai parameter untuk kontrol ini dari `1.32` ke. `1.33` Dukungan standar untuk Kubernetes versi 1.32 di Amazon EKS berakhir pada 23 Maret 2026.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
3 April 2026	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 parameter untuk runtime yang didukung tidak lagi disertakan `ruby3.2` karena Lambda telah menghentikan runtime ini.
Maret 24, 2026	[RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan	Security Hub CSPM memperbarui judul kontrol untuk mencerminkan bahwa kontrol memeriksa semua cluster DB RDS.
Maret 24, 2026	[ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root	Security Hub CSPM memperbarui judul kontrol dan deskripsi untuk mencerminkan bahwa kontrol memeriksa definisi tugas ECS. Security Hub CSPM juga memperbarui kontrol agar tidak menghasilkan temuan untuk definisi tugas yang `runtimePlatform` dikonfigurasi untuk menentukan keluarga `WINDOWS_SERVER` OS.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
9 Maret, 2026	[AppSync.1] C AWS AppSync ache API harus dienkripsi saat diam	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari standar F AWS oundation al Security Best Practices (FSBP). AWS AppSync sekarang menyediak an enkripsi default pada semua cache API saat ini dan yang akan datang.
9 Maret, 2026	[AppSync.6] C AWS AppSync ache API harus dienkripsi saat transit	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari standar F AWS oundation al Security Best Practices (FSBP). AWS AppSync sekarang menyediak an enkripsi default pada semua cache API saat ini dan yang akan datang.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 4, 2026	[ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari standar F AWS oundation al Security Best Practices (FSBP) dan standar NIS T SP 800-53 Rev. 5.
Februari 5, 2026	[AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat	Security Hub CSPM akan menghenti kan kontrol ini dan menghapus dari semua standar CSPM Security Hub yang berlaku pada 9 Maret 2026. AWS AppSync menyediakan enkripsi default pada semua cache API saat ini dan yang akan datang.
Februari 5, 2026	[AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit	Security Hub CSPM akan menghenti kan kontrol ini dan menghapus dari semua standar CSPM Security Hub yang berlaku pada 9 Maret 2026. AWS AppSync menyediakan enkripsi default pada semua cache API saat ini dan yang akan datang.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Januari 16, 2026	[ECS.1] Definisi tugas Amazon ECS harus memiliki mode jaringan yang aman dan definisi pengguna	Security Hub CSPM memberikan pemberitahuan bahwa kontrol ini akan dihentikan dan dihapus dari semua standar CSPM Hub Keamanan yang berlaku setelah 16 Februari 2026.
Januari 12, 2026	[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit	Security Hub CSPM memperbarui kontrol ini untuk menghapus parameter. `loggingEnabled`

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Januari 12, 2026	[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis	Security Hub CSPM menghentikan kontrol dan menghapus kontrol dari semua standar yang berlaku. Security Hub CSPM menghentikan kontrol karena persyaratan Amazon MQ untuk peningkatan versi minor otomatis. Sebelumnya, kontrol diterapkan pada standar F AWS oundational Security Best Practices (FSBP), standar NIST SP 800-53 Rev. 5 dan standar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Januari 12, 2026	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah pengaturan runtime untuk suatu AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `dotnet10` sebagai nilai parameter untuk kontrol ini. AWS Lambda menambahkan dukungan untuk runtime ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Desember 15, 2025	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah pengaturan runtime untuk suatu AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM tidak lagi mendukung `python3.9` sebagai nilai parameter untuk kontrol ini. AWS Lambda tidak lagi mendukung runtime ini.
Desember 12, 2025	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon EKS berjalan pada versi Kubernetes yang didukung. Security Hub CSPM mengubah nilai parameter untuk kontrol ini dari `1.31` ke. `1.32` Dukungan standar untuk Kubernetes versi 1.31 di Amazon EKS berakhir pada 26 November 2025.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 21, 2025	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah pengaturan runtime untuk suatu AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `nodejs24.x` dan `python3.14` sebagai nilai parameter untuk kontrol ini. AWS Lambda menambahkan dukungan untuk runtime ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
14 November 2025	[EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik	Security Hub CSPM memperbarui deskripsi dan alasan untuk kontrol ini. Sebelumnya, kontrol hanya memeriksa penetapan otomatis IP publik IPv4 di subnet Amazon VPC menggunakan flag. `MapPublicIpOnLaunch` Kontrol ini sekarang memeriksa penugasan otomatis IP publik IPv4 dan IPv6. Deskripsi dan alasan kontrol telah diperbarui untuk mencerminkan perubahan ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
14 November 2025	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah pengaturan runtime untuk suatu AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `java25` sebagai nilai parameter untuk kontrol ini. AWS Lambda menambahkan dukungan untuk runtime ini.
November 13, 2025	[SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `HIGH` menjadi. `CRITICAL` Mengizinkan akses publik ke topik Amazon SNS menimbulkan risiko keamanan yang signifikan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 13, 2025	[SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `HIGH` menjadi. `CRITICAL` Mengizinkan akses publik ke antrian Amazon SQS menimbulkan risiko keamanan yang signifikan.
November 13, 2025	[GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `MEDIUM` menjadi. `HIGH` Jenis pemantauan runtime ini menyediakan deteksi ancaman yang ditingkatkan untuk sumber daya Amazon EKS.
November 13, 2025	[MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `LOW` menjadi. `MEDIUM` Upgrade versi minor termasuk patch keamanan yang diperlukan untuk menjaga keamanan broker Amazon MQ.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 13, 2025	[Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `LOW` menjadi. `MEDIUM` Pembaruan perangkat lunak termasuk patch keamanan yang diperlukan untuk menjaga keamanan OpenSearch domain.
November 13, 2025	[RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `LOW` menjadi. `MEDIUM` Perlindun gan penghapus an membantu mencegah penghapus an database Amazon RDS secara tidak sengaja dan penghapusan database RDS oleh entitas yang tidak sah.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 13, 2025	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `LOW` menjadi. `MEDIUM` AWS CloudTrail data logging di Amazon CloudWatch Logs dapat digunakan untuk aktivitas audit, alarm, dan operasi keamanan penting lainnya.
November 13, 2025	[ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `HIGH` menjadi. `MEDIUM` Ber AWS Service Catalog bagi portofolio dengan akun tertentu bisa disengaja dan tidak selalu menunjukkan bahwa portofolio dapat diakses publik.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 13, 2025	[CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `MEDIUM` menjadi. `LOW` Nama `cloudfront.net` domain default untuk CloudFront distribusi Amazon dihasilkan secara acak, yang mengurangi risiko keamanan.
November 13, 2025	[ELB.7] Classic Load Balancer harus mengaktifkan pengeringan koneksi	Security Hub CSPM mengubah tingkat keparahan kontrol ini dari `MEDIUM` menjadi. `LOW` Dalam penerapan multi-instance, instans sehat lainnya dapat menangani sesi pengguna saat instance dihentikan tanpa menguras koneksi, yang mengurangi dampak operasional dan risiko ketersediaan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 13, 2025	[RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default	Security Hub CSPM memperbarui kontrol ini untuk menghapus parameter opsional `validAdminUserNames` .
Oktober 23, 2025	[ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis	Security Hub CSPM mengembalikan perubahan yang dibuat pada judul, deskripsi, dan aturan untuk kontrol ini pada 14 Oktober 2025.
Oktober 22, 2025	[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	Security Hub CSPM memperbarui kontrol ini agar tidak menghasilkan temuan untuk CloudFront distribusi Amazon yang menggunakan asal khusus.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Oktober 16, 2025	[CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan	Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk menggunakan kebijakan keamanan TLS yang direkomendasikan. Security Hub CSPM sekarang mendukung `TLSv1.2_2025` dan `TLSv1.3_2025` sebagai nilai parameter untuk kontrol ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Oktober 14, 2025	[ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis	Security Hub CSPM mengubah judul, deskripsi, dan aturan untuk kontrol ini. Sebelumnya, kontrol memeriksa cluster Redis OSS dan semua grup replikasi, menggunakan aturan elasticac he-redis-cluster-automatic-backup-check. Judul kontrolnya adalah: Cluster ElastiCac he (Redis OSS) harus mengaktifkan cadangan otomatis. Kontrol ini sekarang memeriksa kluster Valkey selain cluster Redis OSS dan semua grup replikasi , menggunakan aturan elas ticache-automatic-backup-ch eck-enabled. Judul dan deskripsi baru mencerminkan bahwa kontrol memeriksa kedua jenis cluster.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Oktober 5, 2025	[Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru	Aturan untuk kontrol ini diperbarui untuk juga menghasilkan tem PASSED uan jika domain OpenSearch Layanan Amazon tidak memiliki pembaruan perangkat lunak yang tersedia dan status pembaruan tidak memenuhi syarat. Sebelumnya, kontrol ini menghasilkan tem PASSED uan hanya jika OpenSearch domain tidak memiliki pembaruan perangkat lunak yang tersedia dan status pembaruan selesai.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
September 24, 2025	[Redshift.9] Cluster Redshift tidak boleh menggunakan nama database default [RedshiftServerless.7] Redshift Serverless namespace tidak boleh menggunakan nama database default	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar yang berlaku. Security Hub CSPM menghentikan kontrol ini karena keterbata san Amazon Redshift yang melekat yang mencegah remediasi `FAILED` temuan yang efektif untuk kontrol. Sebelumnya, kontrol diterapkan pada standar F AWS oundational Security Best Practices (FSBP) dan standar NIST SP 800-53 Rev. 5. Redshift.9 Kontrol juga diterapkan pada standar yang AWS Control Tower dikelola layanan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
9 September 2025	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah pengaturan runtime untuk suatu AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM tidak lagi mendukung `nodejs18.x` sebagai nilai parameter untuk kontrol ini. AWS Lambda tidak lagi mendukung Node.js 18 runtime.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Agustus 13, 2025	[SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan	Security Hub CSPM mengubah judul dan deskripsi kontrol ini. Judul dan deskripsi baru lebih akurat mencerminkan bahwa kontrol memeriksa pengaturan untuk `EnableNetworkIsolation` parameter model yang di SageMaker hosting Amazon AI. Sebelumnya, judul kontrol ini adalah: SageMaker models should block inbound traffic.
Agustus 13, 2025	[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan	Security Hub CSPM mengubah judul dan deskripsi kontrol ini. Judul dan deskripsi baru lebih tepat mencerminkan ruang lingkup dan sifat pemeriksaan yang dilakukan kontrol. Sebelumnya, judul kontrol ini adalah: EFS mount targets should not be associated with a public subnet.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juli 24, 2025	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon EKS berjalan pada versi Kubernetes yang didukung. Security Hub CSPM mengubah nilai parameter untuk kontrol ini dari `1.30` ke. `1.31` Dukungan standar untuk Kubernetes versi 1.30 di Amazon EKS berakhir pada 23 Juli 2025.
Juli 23, 2025	[EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir	Security Hub CSPM mengubah judul kontrol ini. Judul baru lebih akurat mencerminkan bahwa kontrol hanya memeriksa permintaan Amazon EC2 Spot Fleet yang menentukan parameter peluncuran. Sebelumnya, judul kontrol ini adalah: EC2 Spot Fleet requests should enable encryption for attached EBS volumes.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juni 30, 2025	[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol	Security Hub CSPM menghapus kontrol ini dari standar PCI DSS v4.0.1. PCI DSS v4.0.1 tidak secara eksplisit memerlukan penggunaan simbol dalam kata sandi.
Juni 30, 2025	[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	Security Hub CSPM menghapus kontrol ini dari standar NIST SP 800-171 Revisi 2. NIST SP 800-171 Revisi 2 tidak secara eksplisit memerlukan periode kedaluwarsa kata sandi 90 hari atau kurang.
Juni 30, 2025	[RDS.16] Cluster Aurora DB harus dikonfigurasi untuk menyalin tag ke snapshot DB	Security Hub CSPM mengubah judul kontrol ini. Judul baru lebih akurat mencerminkan bahwa kontrol hanya memeriksa cluster Amazon Aurora DB. Sebelumnya, judul kontrol ini adalah: RDS DB clusters should be configured to copy tags to snapshots.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juni 30, 2025	[SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung	Kontrol ini memeriksa apakah instance notebook Amazon SageMaker AI dikonfigurasi untuk berjalan pada platform yang didukung, berdasarkan pengidentifikasi platform yang ditentukan untuk instance notebook. Security Hub CSPM tidak lagi mendukung `notebook-al2-v1` dan `notebook-al2-v2` sebagai nilai parameter untuk kontrol ini. Instans notebook yang berjalan di platform ini mencapai akhir dukungan pada 30 Juni 2025.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
30 Mei 2025	[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	Security Hub CSPM menghapus kontrol ini dari standar PCI DSS v4.0.1. Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM memenuhi persyaratan minimum, termasuk panjang kata sandi minimum 7 karakter. PCI DSS v4.0.1 sekarang membutuhkan kata sandi untuk memiliki minimal 8 karakter. Kontrol terus berlaku untuk standar PCI DSS v3.2.1, yang memiliki persyaratan kata sandi berbeda. Untuk mengevalu asi kebijakan kata sandi akun terhadap persyaratan PCI DSS v4.0.1, Anda dapat menggunakan kontrol. IAM.7 Kontrol ini mengharuskan kata sandi memiliki minimal 8 karakter. Ini juga mendukung nilai kustom untuk panjang kata sandi dan

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
		parameter lainnya. IAM.7Kontrol adalah bagian dari standar PCI DSS v4.0.1 di Security Hub CSPM.
8 Mei 2025	[RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet	Security Hub CSPM memutar kembali pelepasan RDS.46 kontrol di semua. Wilayah AWS Sebelumnya, kontrol ini mendukung standar F AWS oundational Security Best Practices (FSBP).

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
7 April 2025	[ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan	Kontrol ini memeriksa apakah pendengar HTTPS untuk Application Load Balancer atau pendengar TLS untuk Network Load Balancer dikonfigurasi untuk mengenkripsi data yang sedang transit dengan menggunakan kebijakan keamanan yang disarankan. Security Hub CSPM sekarang mendukung dua nilai parameter tambahan untuk kontrol ini: `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` dan. `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04`

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 27, 2025	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah pengaturan runtime untuk suatu AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `ruby3.4` sebagai nilai parameter untuk kontrol ini. AWS Lambda menambahkan dukungan untuk runtime ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 26, 2025	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Untuk `oldestVersionSupported` parameter, Security Hub CSPM mengubah nilai dari `1.29` ke. `1.30` Versi Kubernetes tertua yang didukung sekarang. `1.30`

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 10, 2025	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Kontrol ini memeriksa apakah pengaturan runtime untuk suatu AWS Lambda fungsi cocok dengan nilai yang diharapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM tidak lagi mendukung `dotnet6` dan `python3.8` sebagai nilai parameter untuk kontrol ini. AWS Lambda tidak lagi mendukung runtime ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
7 Maret 2025	[RDS.18] Instans RDS harus digunakan dalam VPC	Security Hub CSPM menghapus kontrol ini dari standar Praktik Terbaik AWS Keamanan Dasar dan pemeriksaan otomatis untuk persyaratan NIST SP 800-53 Rev. 5. Sejak EC2-Class ic jaringan Amazon dihentikan, instans Amazon Relationa l Database Service (Amazon RDS) tidak dapat lagi digunakan di luar VPC.
Januari 10, 2025	[Glue.2] AWS Pekerjaan lem harus mengaktif kan logging	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar.
Desember 20, 2024	EC2.61 melalui EC2.169	Security Hub CSPM memutar kembali rilis kontrol EC2.61 through EC2.169.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Desember 12, 2024	[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database	RDS.23 memeriksa apakah cluster atau instans Amazon Relational Database Service (Amazon RDS) menggunakan port selain port default mesin database. Kami memperbarui kontrol sehingga AWS Config aturan yang mendasarinya mengembalikan hasil `NOT_APPLICABLE` untuk instance RDS yang merupakan bagian dari cluster.
Desember 2, 2024	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `nodejs22.x` sebagai parameter.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 26, 2024	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung sekarang`1.29`.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
20 November 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Config.1 memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifkan. Security Hub CSPM meningkatkan tingkat keparahan kontrol ini dari `MEDIUM` ke. `CRITICAL` Security Hub CSPM juga menambahkan kode status baru dan alasan status untuk temuan yang gagal Config.1 . Perubahan ini mencerminkan pentingnya pen Config.1 goperasia n kontrol CSPM Security Hub. Jika perekaman sumber AWS Config daya dinonaktifkan, Anda dapat menerima temuan kontrol yang tidak akurat. Untuk menerima tem `PASSED` uan untuk Config.1, aktifkan perekaman sumber

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
		daya untuk sumber daya yang sesuai dengan kontrol CSPM Security Hub yang diaktifkan, dan nonaktifkan kontrol yang tidak diperluka n di organisas i Anda. Untuk petunjuk tentang cara mengonfigurasi AWS Config untuk Security Hub CSPM, lihat. Mengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM Untuk daftar kontrol CSPM Security Hub dan sumber daya yang sesuai, lihat. DiperlukanAWS Configsumber daya untuk temuan kontrol

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
November 12, 2024	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `python3.13` sebagai parameter.
Oktober 11, 2024	ElastiCache kontrol	Mengubah judul kontrol untuk ElastiCache.3, ElastiCache.4, ElastiCache.5, dan ElastiCache.7. Judul tidak lagi menyebutkan Redis OSS karena kontrol juga berlaku ElastiCache untuk Valkey.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
September 27, 2024	[ELB.4] Application Load Balancer harus dikonfigurasi untuk menghapus header http yang tidak valid	Judul kontrol yang diubah dari Application Load Balancer harus dikonfigurasi untuk melepaskan header http ke Application Load Balancer harus dikonfigurasi untuk menghapus header http yang tidak valid.
Agustus 19, 2024	Perubahan judul DMS.12 dan ElastiCache kontrol	Mengubah judul kontrol untuk DMS.12 dan sel ElastiCache.1 amanya ElastiCache.7. Kami mengubah judul ini untuk mencerminkan perubahan nama dalam layanan Amazon ElastiCache (Redis OSS).

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Agustus 15, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Config.1 memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifka n. Security Hub CSPM menambahk an parameter kontrol khusus bernama. `includeConfigServiceLinkedRoleCheck` Dengan menyetel parameter ini `kefalse`, Anda dapat memilih untuk tidak memeriksa apakah AWS Config menggunakan peran yang ditautkan layanan.
Juli 31, 2024	[IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai	Judul kontrol yang diubah dari profil AWS IoT Core keamanan harus ditandai ke profil AWS IoT Device Defender keamanan harus ditandai.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juli 29, 2024	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM tidak lagi mendukung `nodejs16.x` sebagai parameter.
Juli 29, 2024	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung adalah`1.28`.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juni 25, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Kontrol ini memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifka n. Security Hub CSPM memperbar ui judul kontrol untuk mencerminkan apa yang dievaluasi kontrol.
Juni 14, 2024	[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log	Kontrol ini memeriksa apakah cluster DB Amazon Aurora MySQL dikonfigu rasi untuk menerbitk an log audit ke Amazon CloudWatc h Logs. Security Hub CSPM memperbarui kontrol sehingga tidak menghasilkan temuan untuk cluster Aurora Serverless v1 DB.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juni 11, 2024	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Kontrol ini memeriksa apakah cluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung adalah`1.27`.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juni 10, 2024	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya	Kontrol ini memeriksa apakah AWS Config diaktifkan dan perekaman AWS Config sumber daya diaktifkan. Sebelumnya, kontrol menghasilkan tem PASSED uan hanya jika Anda mengonfigurasi perekaman untuk semua sumber daya. Security Hub CSPM memperbarui kontrol untuk menghasilkan tem PASSED uan saat perekaman diaktifkan untuk sumber daya yang diperlukan untuk kontrol yang diaktifkan. Kontrol juga telah diperbarui untuk memeriksa apakah peran AWS Config terkait layanan digunakan, yang memberikan izin untuk merekam sumber daya yang diperlukan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
8 Mei 2024	[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA	Kontrol ini memeriksa apakah bucket berversi tujuan umum Amazon S3 mengaktifkan penghapusan autentikasi multi-faktor (MFA). Sebelumnya, kontrol menghasilkan temuan `FAILED` untuk bucket yang memiliki konfigurasi Siklus Hidup. Namun, penghapusan MFA dengan pembuatan versi tidak dapat diaktifkan pada bucket yang memiliki konfigurasi Siklus Hidup. Security Hub CSPM memperbarui kontrol agar tidak menghasilkan temuan untuk bucket yang memiliki konfigurasi Siklus Hidup. Deskripsi kontrol telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
2 Mei 2024	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub CSPM memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh cluster Amazon EKS untuk menghasilkan temuan yang diteruskan. Versi tertua yang didukung saat ini adalah Kubernetes`1.26`.
April 30, 2024	[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan	Judul kontrol yang diubah dari CloudTrail harus diaktifkan menjadi Setidaknya satu CloudTrail jejak harus diaktifkan. Kontrol ini saat ini menghasilkan `PASSED` temuan Akun AWS jika setidaknya satu CloudTrail jejak diaktifkan. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 29, 2024	[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB	Judul kontrol yang diubah dari grup Auto Scaling yang terkait dengan Classic Load Balancer harus menggunakan pemeriksaan kesehatan penyeimbang beban ke grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB. Kontrol ini saat ini mengevaluasi Application, Gateway, Network, dan Classic Load Balancers. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 19, 2024	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis	Kontrol memeriksa apakah AWS CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup peristiwa manajemen baca dan tulis. Sebelumnya, kontrol salah menghasilkan PASSED temuan ketika akun telah di CloudTrail aktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah, bahkan jika tidak ada jejak yang menangkap peristiwa manajemen baca dan tulis. Kontrol sekarang menghasilkan tem PASSED uan hanya ketika CloudTrail diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang menangkap peristiwa manajemen baca dan tulis.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 10, 2024	[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Workgroup Athena mengirim log ke bucket Amazon Simple Storage Service (Amazon S3). Amazon S3 sekarang menyediakan enkripsi default dengan kunci terkelola S3 (SS3-S3) pada bucket S3 baru dan yang sudah ada.
April 10, 2024	[AutoScaling.4] Konfigurasi peluncuran grup Penskalaan Otomatis tidak boleh memiliki batas hop respons metadata lebih besar dari 1	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Batas lompatan respons metadata untuk instans Amazon Elastic Compute Cloud (Amazon EC2) bergantung pada beban kerja.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 10, 2024	[CloudFormation.1] tumpu CloudFormation kan harus diintegrasikan dengan Layanan Pemberitahuan Sederhana (SNS)	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Meng AWS CloudForm ation integrasikan tumpukan dengan topik Amazon SNS bukan lagi praktik terbaik keamanan. Meskipun menginteg rasikan CloudForm ation tumpukan penting dengan topik SNS dapat berguna, itu tidak diperluka n untuk semua tumpukan.
April 10, 2024	[CodeBuild.5] lingkungan CodeBuild proyek seharusnya tidak mengaktifkan mode istimewa	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Mengaktifkan mode istimewa dalam CodeBuild proyek tidak menimbulkan risiko tambahan pada lingkungan pelanggan .

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 10, 2024	[IAM.20] Hindari penggunaan pengguna root	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Tujuan dari kontrol ini ditutupi oleh kontrol lain,[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”.
April 10, 2024	[SNS.2] Pencatatan status pengiriman harus diaktifkan untuk pesan notifikasi yang dikirim ke topik	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Pencatata n status pengirima n untuk topik SNS bukan lagi praktik terbaik keamanan. Meskipun mencatat status pengirima n untuk topik SNS penting dapat berguna, itu tidak diperlukan untuk semua topik.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 10, 2024	[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	Security Hub CSPM menghapus kontrol ini dari Praktik Terbaik AWS dan Service-Managed Standar Keamanan Dasar:. AWS Control Tower Tujuan dari kontrol ini dicakup oleh dua kontrol lain: [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup dan[S3.14] Bucket tujuan umum S3 harus mengaktif kan pembuatan versi. Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 10, 2024	[S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa	Security Hub CSPM menghapus kontrol ini dari Praktik Terbaik AWS dan Service-Managed Standar Keamanan Dasar:. AWS Control Tower Meskipun ada beberapa kasus di mana notifikas i peristiwa untuk bucket S3 berguna, ini bukan praktik terbaik keamanan universal . Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 10, 2024	[SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakanAWS KMS	Security Hub CSPM menghapus kontrol ini dari Praktik Terbaik AWS dan Service-Managed Standar Keamanan Dasar:. AWS Control Tower Secara default, SNS mengenkripsi topik yang diam dengan enkripsi disk. Untuk informasi selengkap nya tentang enkripsi saat istirahat, lihat. Menggunakan AWS KMS untuk mengenkri psi topik tidak lagi direkomendasikan sebagai praktik terbaik keamanan. Kontrol ini masih merupakan bagian dari NIST SP 800-53 Rev. 5.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
8 April 2024	[ELB.6] Aplikasi, Gateway, dan Penyeimbang Beban Jaringan harus mengaktifkan perlindungan penghapusan	Judul kontrol yang diubah dari perlindungan penghapusan Application Load Balancer harus diaktifkan menjadi Application, Gateway, dan Network Load Balancers harus mengaktifkan perlindungan penghapusan. Kontrol ini saat ini mengevaluasi Application, Gateway, dan Network Load Balancers. Judul dan deskripsi telah diubah untuk secara akurat mencerminkan perilaku saat ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 22, 2024	[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	Judul kontrol yang diubah dari Koneksi ke OpenSearch domain harus dienkripsi menggunakan TLS 1.2 menjadi Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru. Sebelumnya, kontrol hanya memeriksa apakah koneksi ke OpenSearch domain menggunakan TLS 1.2. Kontrol sekarang menghasilkan tem `PASSED` uan apakah OpenSearch domain dienkripsi menggunakan kebijakan keamanan TLS terbaru. Judul kontrol dan deskripsi telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 22, 2024	[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru	Judul kontrol yang diubah dari Koneksi ke domain Elasticsearch harus dienkripsi menggunakan TLS 1.2 ke Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru. Sebelumnya, kontrol hanya memeriksa apakah koneksi ke domain Elasticsearch menggunakan TLS 1.2. Kontrol sekarang menghasilkan tem PASSED uan jika domain Elasticsearch dienkripsi menggunakan kebijakan keamanan TLS terbaru. Judul kontrol dan deskripsi telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok	Judul yang diubah dari setelan Akses Publik Blok S3 harus diaktifkan ke bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik	Judul yang diubah dari bucket S3 harus melarang akses baca publik ke bucket tujuan umum S3 harus memblokir akses baca publik. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik	Judul yang diubah dari bucket S3 harus melarang akses tulis publik ke bucket tujuan umum S3 harus memblokir akses tulis publik. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS	Judul yang diubah dari bucket S3 harus memerlukan permintaan untuk menggunakan Secure Socket Layer ke bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan SSL. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	Judul yang diubah dari izin S3 yang diberikan kepada kebijakan bucket lainnya Akun AWS harus dibatasi ke kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah	Judul yang diubah dari bucket S3 harus mengaktifkan replikasi lintas wilayah ke bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah	Judul yang diubah dari bucket S3 harus mengaktifkan replikasi lintas wilayah ke bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.8] Bucket tujuan umum S3 harus memblokir akses publik	Judul yang diubah dari setelan Akses Publik Blok S3 harus diaktifkan di tingkat bucket menjadi bucket tujuan umum S3 harus memblokir akses publik. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.9] Bucket tujuan umum S3 harus mengaktifkan logging akses server	Judul yang diubah dari logging akses server bucket S3 harus diaktifkan menjadi Logging akses server harus diaktifkan untuk bucket tujuan umum S3. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup	Judul yang diubah dari bucket S3 dengan versi diaktifkan harus memiliki kebijakan siklus hidup yang dikonfigurasi ke bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa	Judul yang diubah dari bucket S3 harus mengaktifkan notifikasi peristiwa ke bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3	Judul yang diubah dari daftar kontrol akses S3 (ACL) tidak boleh digunakan untuk mengelola akses pengguna ke bucket ke ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup	Judul yang diubah dari bucket S3 harus memiliki kebijakan siklus hidup yang dikonfigurasi ke bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.14] Bucket tujuan umum S3 harus mengaktifkan pembuatan versi	Judul yang diubah dari bucket S3 harus menggunakan versi ke bucket tujuan umum S3 harus mengaktifkan pembuatan versi. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 12, 2024	[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock	Judul yang diubah dari bucket S3 harus dikonfigurasi untuk menggunakan Object Lock ke bucket tujuan umum S3 harus mengaktifkan Object Lock. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.
Maret 12, 2024	[S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys	Judul yang diubah dari bucket S3 harus dienkripsi saat AWS KMS keys diam dengan bucket tujuan umum S3 harus dienkripsi saat istirahat AWS KMS keys. Security Hub CSPM mengubah judul untuk memperhitungkan jenis bucket S3 baru.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Maret 7, 2024	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `nodejs20.x` dan `ruby3.3` sebagai parameter.
Februari 22, 2024	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `dotnet8` sebagai parameter.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Februari 5, 2024	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub CSPM memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh cluster Amazon EKS untuk menghasilkan temuan yang diteruskan. Versi tertua yang didukung saat ini adalah Kubernetes`1.25`.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
10 Januari 2024	[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif	Judul yang diubah dari CodeBuild GitHub atau URL repositori sumber Bitbucket harus menggunakan OAuth ke URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredenSIAL sensitif. Security Hub CSPM menghapus penyebutan OAuth karena metode koneksi lain juga dapat aman. Security Hub CSPM menghapus penyebutan GitHub karena tidak mungkin lagi memiliki token akses pribadi atau nama pengguna dan kata sandi di URL repositori GitHub sumber.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
8 Januari 2024	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM tidak lagi mendukung `go1.x` dan `java8` sebagai parameter karena ini adalah runtime yang dihentikan.
Desember 29, 2023	[RDS.8] Instans DB RDS harus mengaktifkan perlindungan penghapusan	RDS.8 memeriksa apakah instance Amazon RDS DB yang menggunakan salah satu mesin database yang didukung memiliki perlindungan penghapusan yang diaktifkan. Security Hub CSPM sekarang mendukung `custom-oracle-ee`,`oracle-ee-cdb`, dan `oracle-se2-cdb` sebagai mesin database.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
22 Desember 2023	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `java21` dan `python3.12` sebagai parameter. Security Hub CSPM tidak lagi mendukung `ruby2.7` sebagai parameter.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
15 Desember 2023	[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi	CloudFront.1 memeriksa apakah CloudFront distribusi Amazon memiliki objek root default yang dikonfigurasi. Security Hub CSPM menurunkan tingkat keparahan kontrol ini dari KRITIS ke TINGGI karena menambahkan objek root default adalah rekomendasi yang bergantung pada aplikasi pengguna dan persyaratan spesifik.
5 Desember 2023	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22	Judul kontrol yang diubah dari grup Keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 ke grup Keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
5 Desember 2023	[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389	Mengubah judul kontrol dari Pastikan tidak ada grup keamanan yang mengizinkan masuk dari 0.0.0. 0/0 ke port 3389 ke grup Keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
5 Desember 2023	[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch	Judul kontrol yang diubah dari logging Database harus diaktifkan ke instans DB RDS harus menerbitkan CloudWatch log ke Log. Security Hub CSPM mengident ifikasi bahwa kontrol ini hanya memeriksa apakah log dipublika sikan ke Amazon Logs dan tidak memeriksa apakah CloudWatch log RDS diaktifkan. Kontrol menghasil kan tem PASSED uan jika instance RDS DB dikonfigurasi untuk menerbitkan CloudWatch log ke Log. Judul kontrol telah diperbarui untuk mencerminkan perilaku saat ini.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
5 Desember 2023	[EKS.8] Cluster EKS harus mengaktifkan logging audit	Kontrol ini memeriksa apakah cluster Amazon EKS mengaktifkan pencatatan audit. A AWS Config turan yang digunakan Security Hub CSPM untuk mengevaluasi kontrol ini diubah dari `eks-cluster-logging-enabled` menjadi. `eks-cluster-log-enabled`

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
17 November 2023	[EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi	EC2.19 memeriksa apakah lalu lintas masuk yang tidak dibatasi untuk grup keamanan dapat diakses ke port tertentu yang dianggap berisiko tinggi. Security Hub CSPM memperbar ui kontrol ini untuk memperhitungkan daftar awalan terkelola ketika mereka diberikan sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan tem `FAILED` uan jika daftar awalan berisi string '0.0.0. 0/0' atau ': :/0'.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
16 November 2023	[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi	Judul kontrol yang diubah dari CloudWatch alarm harus memiliki tindakan yang dikonfigurasi untuk status ALARM ke CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi.
16 November 2023	[CloudWatch.16] CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu	Judul kontrol yang diubah dari grup CloudWatch log harus dipertahankan setidaknya selama 1 tahun agar grup CloudWatch log harus dipertahankan untuk jangka waktu tertentu.
16 November 2023	[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan	Judul kontrol yang diubah dari fungsi VPC Lambda harus beroperasi di lebih dari satu Zona Ketersediaan menjadi fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
16 November 2023	[AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan	Judul kontrol yang diubah dari AWS AppSync seharusny a pencatatan tingkat permintaan dan tingkat bidang diaktifkan AWS AppSync harus mengaktifkan logging tingkat bidang.
16 November 2023	[EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik	Judul kontrol yang diubah dari node master MapReduce cluster Amazon Elastic seharusny a tidak memiliki alamat IP publik ke node utama cluster Amazon EMR seharusnya tidak memiliki alamat IP publik.
16 November 2023	[Opensearch.2] OpenSearch domain seharusny a tidak dapat diakses publik	Judul kontrol yang diubah dari OpenSearch domain harus berada di VPC ke OpenSearch domain tidak boleh diakses publik.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
16 November 2023	[ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik	Judul kontrol yang diubah dari domain Elasticsearch harus berada di VPC ke domain Elasticsearch seharusnya tidak dapat diakses publik.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
31 Oktober 2023	[ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan	ES.4 memeriksa apakah domain Elasticsearch dikonfigurasi untuk mengirim log kesalahan ke Amazon CloudWatch Logs. Kontrol sebelumnya menghasilkan temuan PASSED untuk domain Elasticsearch yang memiliki log apa pun yang dikonfigurasi untuk dikirim ke CloudWatch Log. Security Hub CSPM memperbarui kontrol untuk menghasilkan temuan PASSED hanya untuk domain Elasticsearch yang dikonfigurasi untuk mengirim log kesalahan ke Log. CloudWatch Kontrol juga diperbarui untuk mengecualikan versi Elasticsearch yang tidak mendukung log kesalahan dari evaluasi.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22	EC2.13 memeriksa apakah grup keamanan mengizinkan akses masuk tanpa batas ke port 22. Security Hub CSPM memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola ketika mereka diberikan sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan tem `FAILED` uan jika daftar awalan berisi string '0.0.0. 0/0' atau ': :/0'.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389	EC2.14 memeriksa apakah grup keamanan mengizinkan akses masuk tanpa batas ke port 3389. Security Hub CSPM memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola ketika mereka diberikan sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan tem `FAILED` uan jika daftar awalan berisi string '0.0.0. 0/0' atau ': :/0'.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
16 Oktober 2023	[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi	EC2.18 memeriksa apakah grup keamanan yang digunakan mengizinkan lalu lintas masuk yang tidak dibatasi. Security Hub CSPM memperbarui kontrol ini untuk memperhitungkan daftar awalan terkelola ketika mereka diberikan sebagai sumber untuk aturan grup keamanan. Kontrol menghasilkan tem `FAILED` uan jika daftar awalan berisi string '0.0.0. 0/0' atau ': :/0'.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
16 Oktober 2023	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `python3.11` sebagai parameter.
4 Oktober 2023	[S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah	Security Hub CSPM menambahkan parameter `ReplicationType` dengan nilai `CROSS-REGION` untuk memastikan bahwa bucket S3 mengaktifkan replikasi lintas wilayah daripada replikasi wilayah yang sama.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
27 September 2023	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	Security Hub CSPM memperbarui versi Kubernetes tertua yang didukung yang dapat dijalankan oleh cluster Amazon EKS untuk menghasilkan temuan yang diteruskan. Versi tertua yang didukung saat ini adalah Kubernetes`1.24`.
20 September 2023	Distri CloudFront.2 CloudFront busi [] harus mengaktifkan identitas akses asal	Security Hub CSPM menghentikan kontrol ini dan menghapusnya dari semua standar. Sebaliknya, gunakan [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal. Kontrol akses asal adalah praktik terbaik keamanan saat ini. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
20 September 2023	[EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus	Security Hub CSPM menghapus kontrol ini dari Praktik Terbaik AWS Keamanan Dasar (FSBP) dan Institut Standar dan Teknologi Nasional (NIST) SP 800-53 Rev. 5. Itu masih bagian dari Service-Managed Standar: AWS Control Tower. Kontrol ini menghasil kan temuan yang diteruskan jika grup keamanan dilampirk an ke instans EC2 atau ke antarmuka jaringan elastis. Namun, untuk kasus penggunaan tertentu, grup keamanan yang tidak terikat tidak menimbulkan risiko keamanan. Anda dapat menggunakan kontrol EC2 lainnya —seperti EC2.2,,, EC2.13 EC2.14 EC2.18, dan EC2.19 —untuk memantau grup keamanan Anda.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
20 September 2023	[EC2.29] Instans EC2 harus diluncurkan dalam VPC	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Amazon EC2 telah memigrasikan EC2-Classic instans ke VPC. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.
20 September 2023	[S3.4] Bucket S3 harus mengaktifkan enkripsi sisi server	Security Hub CSPM menghentikan kontrol ini dan menghapus nya dari semua standar. Amazon S3 sekarang menyediak an enkripsi default dengan kunci terkelola S3 (SS3-S3) pada bucket S3 baru dan yang sudah ada. Pengaturan enkripsi tidak berubah untuk bucket yang ada yang dienkripsi dengan SS3-S3 atau enkripsi SS3-KMS sisi server. Kontrol ini akan dihapus dari dokumentasi dalam 90 hari.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
14 September 2023	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar	Judul kontrol yang diubah dari Grup keamanan default VPC seharusnya tidak mengizinkan lalu lintas masuk dan keluar ke grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar.
14 September 2023	[IAM.9] MFA harus diaktifkan untuk pengguna root	Judul kontrol yang diubah dari MFA Virtual harus diaktifkan untuk pengguna root ke MFA harus diaktifkan untuk pengguna root.
14 September 2023	[RDS.19] Langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa cluster kritis	Judul kontrol yang diubah dari Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa cluster kritis menjadi Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa cluster kritis.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
14 September 2023	[RDS.20] Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting	Judul kontrol yang diubah dari Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa instans database penting ke Langganan notifikasi peristiwa RDS yang ada harus dikonfigu rasi untuk peristiwa instance database penting.
14 September 2023	[WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat	Judul kontrol yang diubah dari Aturan Regional WAF harus memiliki setidaknya satu syarat menjadi aturan Regional AWS WAF Klasik harus memiliki setidaknya satu kondisi.
14 September 2023	[WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan	Judul kontrol yang diubah dari Grup aturan regional WAF harus memiliki setidaknya satu aturan ke Grup aturan Regional AWS WAF Klasik harus memiliki setidaknya satu aturan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
14 September 2023	[WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan	Judul kontrol yang diubah dari ACL web regional WAF harus memiliki setidaknya satu aturan atau grup aturan menjadi ACL web regional AWS WAF Klasik harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat	Judul kontrol yang diubah dari Aturan global WAF harus memiliki setidaknya satu kondisi menjadi aturan global AWS WAF klasik harus memiliki setidaknya satu kondisi.
14 September 2023	[WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan	Judul kontrol yang diubah dari Grup aturan global WAF harus memiliki setidaknya satu aturan ke Grup aturan global AWS WAF klasik harus memiliki setidaknya satu aturan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
14 September 2023	[WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan	Judul kontrol yang diubah dari ACL web global WAF harus memiliki setidakny a satu aturan atau grup aturan menjadi ACL web global AWS WAF klasik harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan	Judul kontrol yang diubah dari ACL web WAFv2 harus memiliki setidakny a satu aturan atau grup aturan ke ACL AWS WAF web harus memiliki setidaknya satu aturan atau grup aturan.
14 September 2023	[WAF.11]AWS WAFpencatatan ACL web harus diaktifkan	Judul kontrol yang diubah dari log ACL web AWS WAF v2 harus diaktifkan ke logging ACL AWS WAF web harus diaktifkan.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juli 20, 2023	[S3.4] Bucket S3 harus mengaktifkan enkripsi sisi server	S3.4 memeriksa apakah bucket Amazon S3 mengaktifkan enkripsi sisi server atau kebijakan bucket S3 secara eksplisit menolak `PutObject` permintaan tanpa enkripsi sisi server. Security Hub CSPM memperbarui kontrol ini untuk menyertakan enkripsi sisi server lapis ganda dengan kunci KMS (). DSSE-KMS Kontrol menghasilkan temuan yang diteruskan ketika bucket S3 dienkripsi dengan SSE-S3, SSE-KMS, atau DSSE-KMS.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Juli 17, 2023	[S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys	S3.17 memeriksa apakah bucket Amazon S3 dienkripsi dengan AWS KMS key. Security Hub CSPM memperbarui kontrol ini untuk menyertakan enkripsi sisi server lapis ganda dengan kunci KMS (). DSSE-KMS Kontrol menghasilkan temuan yang diteruskan ketika bucket S3 dienkripsi dengan SSE-KMS atau DSSE-KMS.
9 Juni 2023	[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung	EKS.2 memeriksa apakah cluster Amazon EKS berjalan pada versi Kubernetes yang didukung. Versi tertua yang didukung sekarang ada. `1.23`

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
9 Juni 2023	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `ruby3.2` sebagai parameter.
Juni 5, 2023	[APIGateway.5] Data cache API REST API Gateway harus dienkripsi saat diam	APIGateway.5.checks apakah semua metode di tahapan API REST API Amazon Gateway dienkripsi saat diam. Security Hub CSPM memperbarui kontrol untuk mengevaluasi enkripsi metode tertentu hanya ketika caching diaktifkan untuk metode tersebut.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
Mei 18, 2023	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `java17` sebagai parameter.
Mei 18, 2023	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM tidak lagi mendukung `nodejs12.x` sebagai parameter.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
April 23, 2023	[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru	ECS.10 memeriksa apakah layanan Amazon ECS Fargate menjalankan versi platform Fargate terbaru. Pelanggan dapat menggunakan Amazon ECS melalui ECS secara langsung, atau dengan menggunakan. CodeDeploy Security Hub CSPM memperbarui kontrol ini untuk menghasilkan temuan Lulus saat Anda menggunakannya CodeDeploy untuk menerapkan layanan ECS Fargate.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
20 April 2023	[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS	S3.6 memeriksa apakah kebijakan bucket Amazon Simple Storage Service (Amazon S3) mencegah prinsipal dari pihak lain Akun AWS melakukan tindakan yang ditolak pada sumber daya di bucket S3. Security Hub CSPM memperbarui kontrol untuk memperhitungkan kondisi dalam kebijakan bucket.
18 April 2023	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM sekarang mendukung `python3.10` sebagai parameter.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
18 April 2023	[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung	Lambda.2 memeriksa apakah pengaturan AWS Lambda fungsi untuk runtime cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Security Hub CSPM tidak lagi mendukung `dotnetcore3.1` sebagai parameter.

Tanggal perubahan	ID kontrol dan judul	Deskripsi perubahan
17 April 2023	[RDS.11] Instans RDS harus mengaktifkan cadangan otomatis	RDS.11 memeriksa apakah instans Amazon RDS mengaktifkan pencadangan otomatis, dengan periode retensi cadangan yang lebih besar dari atau sama dengan tujuh hari. Security Hub CSPM memperbar ui kontrol ini untuk mengecualikan replika baca dari evaluasi, karena tidak semua mesin mendukung pencadangan otomatis pada replika baca. Selain itu, RDS tidak menyediakan opsi untuk menentuka n periode retensi cadangan saat membuat replika baca. Replika baca dibuat dengan periode retensi cadangan secara `0` default.

Kontrol CSPM Security Hub untukAkun AWS

Kontrol CSPM Security Hub ini mengevaluasi. Akun AWS

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.2, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`security-account-information-provided`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akun Amazon Web Services (AWS) memiliki informasi kontak keamanan. Kontrol gagal jika informasi kontak keamanan tidak disediakan untuk akun.

Kontak keamanan alternatif memungkinkan AWS untuk menghubungi orang lain tentang masalah dengan akun Anda jika Anda tidak tersedia. Pemberitahuan dapat berasal dariDukungan, atau Layanan AWS tim lain tentang topik terkait keamanan yang terkait dengan penggunaan Anda. Akun AWS

Remediasi

Untuk menambahkan kontak alternatif sebagai kontak keamanan ke kontak AndaAkun AWS, lihat Memperbarui kontak alternatif untuk Anda Akun AWS di Panduan Referensi Manajemen AWS Akun.

[Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`account-part-of-organizations`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa Akun AWS apakah suatu bagian dari organisasi yang dikelola melaluiAWS Organizations. Kontrol gagal jika akun bukan bagian dari organisasi.

Organizations membantu Anda mengelola lingkungan secara terpusat saat Anda meningkatkan beban kerja. AWS Anda dapat menggunakan beberapa Akun AWS untuk mengisolasi beban kerja yang memiliki persyaratan keamanan tertentu, atau untuk mematuhi kerangka kerja seperti HIPAA atau PCI. Dengan membuat organisasi, Anda dapat mengelola beberapa akun sebagai satu unit dan mengelola aksesLayanan AWS, sumber daya, dan Wilayah secara terpusat.

Remediasi

Untuk membuat organisasi baru dan Akun AWS menambahkannya secara otomatis, lihat Membuat organisasi di Panduan AWS Organizations Pengguna. Untuk menambahkan akun ke organisasi yang ada, lihat Mengundang Akun AWS untuk bergabung dengan organisasi Anda di Panduan AWS Organizations Pengguna.

Kontrol CSPM Security Hub untukAWS Amplify

Kontrol CSPM Security Hub ini mengevaluasi AWS Amplify layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Amplify.1] Amplify aplikasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Amplify::App`

AWS Configaturan: amplify-app-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Amplify aplikasi memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika aplikasi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya akan memeriksa keberadaan kunci tag dan gagal jika aplikasi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Amplify aplikasi, lihat Dukungan penandaan sumber daya di Panduan Pengguna AWS Amplify Hosting.

[Amplify.2] Amplify branch harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Amplify::Branch`

AWS Configaturan: amplify-branch-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Amplify cabang memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika cabang tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cabang tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu

Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Amplify cabang, lihat Dukungan penandaan sumber daya di Panduan Pengguna AWS Amplify Hosting.

Kontrol CSPM Hub Keamanan untuk Amazon API Gateway

AWS Security Hub CSPM Kontrol ini mengevaluasi layanan dan sumber daya Amazon API Gateway. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[APIGateway.1] API Gateway REST dan logging eksekusi WebSocket API harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

AWS Config aturan: api-gw-execution-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`loggingLevel`	Tingkat pencatatan log	Enum	`ERROR`, `INFO`	`No default value`

Kontrol ini memeriksa apakah semua tahapan Amazon API Gateway REST atau WebSocket API mengaktifkan logging. Kontrol gagal jika tidak `loggingLevel` `ERROR` atau `INFO` untuk semua tahapan API. Kecuali Anda memberikan nilai parameter khusus untuk menunjukkan bahwa jenis log tertentu harus diaktifkan, Security Hub CSPM menghasilkan temuan yang diteruskan jika tingkat logging adalah salah satu atau`ERROR`. `INFO`

Tahap REST atau WebSocket API Gateway API harus mengaktifkan log yang relevan. API Gateway REST dan logging eksekusi WebSocket API menyediakan catatan rinci permintaan yang dibuat ke API Gateway REST dan tahapan WebSocket API. Tahapannya meliputi respons backend integrasi API, respons otorizer Lambda, dan titik akhir `requestId` untuk AWS integrasi.

Remediasi

Untuk mengaktifkan logging untuk operasi REST dan WebSocket API, lihat Mengatur CloudWatch pencatatan API menggunakan konsol API Gateway di Panduan Pengembang API Gateway.

[APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: api-gw-ssl-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahap API REST API Amazon API Gateway memiliki sertifikat SSL yang dikonfigurasi. Sistem backend menggunakan sertifikat ini untuk mengotentikasi bahwa permintaan masuk berasal dari API Gateway.

Tahap API REST API Gateway harus dikonfigurasi dengan sertifikat SSL untuk memungkinkan sistem backend mengotentikasi permintaan yang berasal dari API Gateway.

Remediasi

Untuk petunjuk terperinci tentang cara membuat dan mengonfigurasi sertifikat SSL API REST API API, lihat Mengh asilkan dan mengonfigurasi sertifikat SSL untuk otentikasi backend di Panduan Pengembang API Gateway.

[APIGateway.3] Tahap API REST API Gateway harus memiliki AWS X-Ray pelacakan diaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-7

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: api-gw-xray-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pelac AWS X-Ray akan aktif diaktifkan untuk tahapan API REST API Amazon API Gateway Anda.

X-Ray penelusuran aktif memungkinkan respons yang lebih cepat terhadap perubahan kinerja di infrastruktur yang mendasarinya. Perubahan kinerja dapat mengakibatkan kurangnya ketersediaan API. X-Raypelacakan aktif menyediakan metrik real-time permintaan pengguna yang mengalir melalui operasi API REST API Gateway dan layanan yang terhubung.

Remediasi

Untuk petunjuk terperinci tentang cara mengaktifkan pelac X-Ray akan aktif untuk operasi API REST API Gateway API, lihat dukungan pelacakan aktif Amazon API Gateway AWS X-Ray di Panduan AWS X-Ray Pengembang.

[APIGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF

Persyaratan terkait: NIST.800-53.r5 AC-4 (21)

Kategori: Melindungi > Layanan perlindungan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: api-gw-associated-with-waf

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahap API Gateway menggunakan daftar kontrol akses AWS WAF web (ACL). Kontrol ini gagal jika ACL AWS WAF web tidak dilampirkan ke tahap REST API Gateway.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan API dari serangan. Ini memungkinkan Anda untuk mengonfigurasi ACL, yang merupakan seperangkat aturan yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan keamanan web yang dapat disesuaikan dan kondisi yang Anda tentukan. Pastikan bahwa tahap API Gateway Anda dikaitkan dengan ACL AWS WAF web untuk membantu melindunginya dari serangan berbahaya.

Remediasi

Untuk informasi tentang cara menggunakan konsol API Gateway untuk mengaitkan ACL web AWS WAF Regional dengan tahap API Gateway API yang ada, lihat Menggunakan AWS WAF untuk melindungi API Anda di Panduan Pengembang API Gateway.

[APIGateway.5] Data cache API REST API Gateway harus dienkripsi saat diam

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Melindungi > Perlindungan data > Enkripsi data saat diam

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::Stage`

AWS Config aturan: `api-gw-cache-encrypted` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah semua metode dalam tahap API REST API Gateway API yang mengaktifkan cache dienkripsi. Kontrol gagal jika ada metode dalam tahap API Gateway REST API yang dikonfigurasi untuk cache dan cache tidak dienkripsi. Security Hub CSPM mengevaluasi enkripsi metode tertentu hanya ketika caching diaktifkan untuk metode tersebut.

Mengenkripsi data saat diam mengurangi risiko data yang disimpan pada disk diakses oleh pengguna yang tidak diautentikasi. AWS Ini menambahkan satu set kontrol akses lain untuk membatasi kemampuan pengguna yang tidak sah mengakses data. Misalnya, izin API diperlukan untuk mendekripsi data sebelum dapat dibaca.

Cache API REST API Gateway harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Untuk mengonfigurasi cache API untuk tahap, lihat Meng aktifkan caching Amazon API Gateway di Panduan Pengembang API Gateway. Di Peng aturan Cache, pilih Enkripsi data cache.

[APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi

Persyaratan terkait: NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Mel indungi > Manajemen Akses Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGatewayV2::Route`

AWS Config aturan: api-gwv2-authorization-type-configured

Jenis jadwal: Ber kala

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`authorizationType`	Jenis otorisasi rute API	Enum	`AWS_IAM`, `CUSTOM`, `JWT`	Tidak ada nilai default

Kontrol ini memeriksa apakah rute Amazon API Gateway memiliki jenis otorisasi. Kontrol gagal jika rute Gateway API tidak memiliki jenis otorisasi apa pun. Secara opsional, Anda dapat memberikan nilai parameter kustom jika Anda ingin kontrol dilewati hanya jika rute menggunakan jenis otorisasi yang ditentukan dalam `authorizationType` parameter.

API Gateway mendukung beberapa mekanisme untuk mengendalikan dan mengelola akses ke API Anda. Dengan menentukan jenis otorisasi, Anda dapat membatasi akses ke API Anda hanya untuk pengguna atau proses yang berwenang.

Remediasi

Untuk mengatur jenis otorisasi untuk API HTTP, lihat Meng ontrol dan mengelola akses ke API HTTP di API Gateway di Panduan Pengembang API Gateway. Untuk mengatur jenis otorisasi untuk WebSocket API, lihat Meng ontrol dan mengelola akses ke WebSocket API di API Gateway di Panduan Pengembang API Gateway.

[APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages

Persyaratan terkait: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGatewayV2::Stage`

AWS Config aturan: api-gwv2-access-logs-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tahap Amazon API Gateway V2 telah mengonfigurasi logging akses. Kontrol ini gagal jika pengaturan log akses tidak ditentukan.

Log akses API Gateway memberikan informasi terperinci tentang siapa yang telah mengakses API Anda dan bagaimana pemanggil mengakses API. Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Aktifkan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah.

Untuk praktik terbaik tambahan, lihat Meman tau REST API di Panduan Pengembang API Gateway.

Remediasi

Untuk mengatur log akses, lihat Meng atur pen CloudWatch catatan API menggunakan konsol API Gateway di Panduan Pengembang API Gateway.

[APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGatewayV2::Integration`

AWS Config aturan: apigatewayv2-integration-private-https-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah integrasi API Gateway V2 mengaktifkan HTTPS untuk koneksi pribadi. Kontrol gagal jika koneksi pribadi tidak memiliki TLS yang dikonfigurasi.

Tautan VPC menghubungkan API Gateway ke sumber daya pribadi. Sementara VPC Links membuat konektivitas pribadi, mereka tidak secara inheren mengenkripsi data. Mengkonfigurasi TLS memastikan penggunaan HTTPS untuk enkripsi ujung ke ujung dari klien melalui API Gateway ke backend. Tanpa TLS, lalu lintas API sensitif mengalir tanpa terenkripsi di seluruh koneksi pribadi. Enkripsi HTTPS melindungi lalu lintas melalui koneksi pribadi dari intersepsi data, serangan man-in-the-middle, dan paparan kredenSIAL.

Remediasi

Untuk mengaktifkan enkripsi saat transit untuk koneksi pribadi dalam Integrasi API Gateway v2, lihat Memperbarui integrasi pribadi di Panduan Pengembang Amazon API Gateway. Konfigur asikan konfigurasi TLS sehingga integrasi pribadi menggunakan protokol HTTPS.

[APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan

Kategori: Mel indungi > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ApiGateway::DomainName`

AWS Config aturan: apigateway-domain-name-tls-check

Jenis jadwal: Perubahan dipicu

Parameter:

- `allowedSecurityPolicies`: `SecurityPolicy_TLS13_1_3_2025_09, SecurityPolicy_TLS13_1_3_FIPS_2025_09, SecurityPolicy_TLS13_1_2_PFS_PQ_2025_09, SecurityPolicy_TLS13_2025_EDGE, SecurityPolicy_TLS12_PFS_2025_EDGE` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah nama domain API Gateway dikonfigurasi untuk mengenkripsi data yang sedang transit dengan menggunakan kebijakan keamanan yang disarankan. Kontrol gagal jika nama domain API Gateway tidak dikonfigurasi untuk menggunakan kebijakan keamanan yang direkomendasikan.

Kontrol ini menghasilkan tem `FAILED` uan untuk nama domain kustom yang dilampirkan ke API HTTP. Jika Anda memiliki kasus penggunaan yang sah untuk API HTTP, Anda dapat menekan temuan tersebut.

Kebijakan keamanan adalah kombinasi standar untuk versi TLS minimum dan cipher suite yang ditawarkan oleh API Gateway. Saat klien Anda membuat handshake TLS ke API atau nama domain kustom Anda, kebijakan keamanan memberlakukan versi TLS dan cipher suite yang diterima oleh API Gateway. Kebijakan keamanan melindungi API dan nama domain kustom Anda dari masalah keamanan jaringan seperti manipulasi dan penyadapan antara klien dan server. Menggunakan

kebijakan keamanan yang direkomendasikan membantu memastikan bahwa nama domain API Gateway menggunakan konfigurasi TLS modern dan aman yang melindungi data yang sedang transit antara klien dan API Anda.

Remediasi

Untuk memperbarui kebijakan keamanan TLS untuk nama domain API Gateway, lihat Cara mengubah kebijakan keamanan di Panduan Pengembang Amazon API Gateway.

Kontrol CSPM Security Hub untukAWS AppConfig

Kontrol CSPM Security Hub ini mengevaluasi AWS AppConfig layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[AppConfig.1]AWS AppConfigaplikasi harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppConfig::Application`

AWS Configaturan: `appconfig-application-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS AppConfig aplikasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika aplikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aplikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke AWS AppConfig aplikasi, lihat TagResourcedi Referensi AWS AppConfig API.

[AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppConfig::ConfigurationProfile`

AWS Configaturan: `appconfig-configuration-profile-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah profil AWS AppConfig konfigurasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika profil konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke profil AWS AppConfig konfigurasi, lihat TagResourcedi Referensi AWS AppConfig API.

[AppConfig.3]AWS AppConfiglingkungan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppConfig::Environment`

AWS Configaturan: `appconfig-environment-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS AppConfig lingkungan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika lingkungan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika

parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika lingkungan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke AWS AppConfig lingkungan, lihat TagResourcedi Referensi AWS AppConfig API.

[AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppConfig::ExtensionAssociation`

AWS Configaturan: `appconfig-extension-association-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah asosiasi AWS AppConfig ekstensi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika asosiasi ekstensi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika asosiasi ekstensi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke asosiasi AWS AppConfig ekstensi, lihat TagResourcedi Referensi AWS AppConfig API.

Kontrol CSPM Security Hub untuk Amazon AppFlow

Kontrol CSPM Security Hub ini mengevaluasi AppFlow layanan dan sumber daya Amazon.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[AppFlow.1] AppFlow Aliran Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppFlow::Flow`

AWS Configaturan: `appflow-flow-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AppFlow aliran Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika aliran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alur tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke AppFlow alur Amazon, lihat Membuat alur di Amazon AppFlow di Panduan AppFlow Pengguna Amazon.

Kontrol CSPM Security Hub untukAWS App Runner

AWS Security Hub CSPMKontrol ini mengevaluasi AWS App Runner layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[AppRunner.1] Layanan Pelari Aplikasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppRunner::Service`

AWS Configaturan: apprunner-service-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS App Runner layanan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika layanan App Runner tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika layanan App Runner tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal

atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS App Runner layanan, lihat TagResourcedi Referensi AWS App Runner API.

[AppRunner.2] Konektor VPC App Runner harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppRunner::VpcConnector`

AWS Configaturan: apprunner-vpc-connector-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah konektor AWS App Runner VPC memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika konektor VPC tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredKeyTags` Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konektor VPC tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk informasi tentang menambahkan tag ke konektor AWS App Runner VPC, lihat TagResourcedi Referensi AWS App RunnerAPI.

Kontrol CSPM Security Hub untukAWS AppSync

Kontrol CSPM Security Hub ini mengevaluasi AWS AppSync layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat

> **Important**
>
> Security Hub CSPM menghentikan kontrol ini pada 9 Maret 2026. Untuk informasi lebih lanjut, lihatLog perubahan untuk kontrol CSPM Security Hub. AWS AppSyncsekarang menyediakan enkripsi default pada semua cache API saat ini dan masa depan.

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Configaturan: appsync-cache-ct-encryption-at-rest

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cache AWS AppSync API dienkripsi saat istirahat. Kontrol gagal jika cache API tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Anda tidak dapat mengubah pengaturan enkripsi setelah mengaktifkan caching untuk API AndaAWS AppSync. Sebagai gantinya, Anda harus menghapus cache dan membuatnya kembali dengan enkripsi diaktifkan. Untuk informasi selengkapnya, lihat Enkripsi cache di Panduan AWS AppSync Pengembang.

[AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan

Persyaratan terkait: PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Configaturan: **`appsync-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub	
`fieldLoggingLevel`	Tingkat pencatatan lapangan	Enum	`ERROR`, `ALL`, `INFO`, `DEBUG`	No `default value`	

Kontrol ini memeriksa apakah AWS AppSync API telah mengaktifkan logging tingkat bidang. Kontrol gagal jika tingkat log penyelesai bidang diatur ke Tidak Ada. Kecuali Anda memberikan nilai parameter khusus untuk menunjukkan bahwa jenis log tertentu harus diaktifkan, Security Hub CSPM menghasilkan temuan yang diteruskan jika tingkat log penyelesai bidang adalah salah satu atau. `ERROR` `ALL`

Anda dapat menggunakan logging dan metrik untuk mengidentifikasi, memecahkan masalah, dan mengoptimalkan kueri GraphQL Anda. Mengaktifkan logging untuk AWS AppSync GraphQL membantu Anda mendapatkan informasi terperinci tentang permintaan dan tanggapan API, mengidentifikasi dan menanggapi masalah, dan mematuhi persyaratan peraturan.

Remediasi

Untuk mengaktifkan pencatatanAWS AppSync, lihat Pengaturan dan konfigurasi di Panduan AWS AppSync Pengembang.

[AppSync.4]AWS AppSyncGraphQL API harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Configaturan: `tagged-appsync-graphqlapi` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS AppSync GraphQL API memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika GraphQL API tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika GraphQL API tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS AppSync GraphQL API, TagResourcelihat di AWS AppSync Referensi API.

[AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AppSync::GraphQLApi`

AWS Configaturan: **`appsync-authorization-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `AllowedAuthorizationTypes: AWS_LAMBDA,AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah aplikasi Anda menggunakan kunci API untuk berinteraksi dengan AWS AppSync GraphQL API. Kontrol gagal jika AWS AppSync GraphQL API diautentikasi dengan kunci API.

Kunci API adalah nilai hard-code dalam aplikasi Anda yang dihasilkan oleh AWS AppSync layanan saat Anda membuat titik akhir GraphQL yang tidak diautentikasi. Jika kunci API ini dikompromikan, titik akhir Anda rentan terhadap akses yang tidak diinginkan. Kecuali Anda mendukung aplikasi

atau situs web yang dapat diakses publik, kami tidak menyarankan menggunakan kunci API untuk otentikasi.

Remediasi

Untuk menetapkan opsi otorisasi untuk AWS AppSync GraphQL API Anda, lihat Otorisasi dan otentikasi di Panduan Pengembang. AWS AppSync

[AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit

> **Important**
>
> Security Hub CSPM menghentikan kontrol ini pada 9 Maret 2026. Untuk informasi lebih lanjut, lihatLog perubahan untuk kontrol CSPM Security Hub. AWS AppSyncsekarang menyediakan enkripsi default pada semua cache API saat ini dan masa depan.

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AppSync::ApiCache`

AWS Configaturan: appsync-cache-ct-encryption-in-transit

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cache AWS AppSync API dienkripsi saat transit. Kontrol gagal jika cache API tidak dienkripsi saat transit.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara klaster Anda dan aplikasi Anda. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Anda tidak dapat mengubah pengaturan enkripsi setelah mengaktifkan caching untuk API AndaAWS AppSync. Sebagai gantinya, Anda harus menghapus cache dan membuatnya kembali dengan

enkripsi diaktifkan. Untuk informasi selengkapnya, lihat Enkripsi cache di Panduan AWS AppSync Pengembang.

Kontrol CSPM Security Hub untuk Amazon Athena

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Athena. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat

> **Important**
>
> Security Hub CSPM menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Log perubahan untuk kontrol CSPM Security Hub.

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Athena::WorkGroup`

AWS Configaturan: athena-workgroup-encrypted-at-rest

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah workgroup Athena dienkripsi saat istirahat. Kontrol gagal jika workgroup Athena tidak dienkripsi saat istirahat.

Di Athena, Anda dapat membuat grup kerja untuk menjalankan kueri untuk tim, aplikasi, atau beban kerja yang berbeda. Setiap workgroup memiliki pengaturan untuk mengaktifkan enkripsi pada semua query. Anda memiliki opsi untuk menggunakan enkripsi sisi server dengan kunci terkelola Amazon Simple Storage Service (Amazon S3), enkripsi sisi server dengan kunci AWS KMS (), atau enkripsi sisi klien AWS Key Management Service dengan kunci KMS yang dikelola pelanggan. Data saat

istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk grup kerja Athena, lihat Mengedit grup kerja di Panduan Pengguna Amazon Athena. Di bagian Konfigurasi Hasil Kueri, pilih Enkripsi hasil kueri.

[Athena.2] Katalog data Athena harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Athena::DataCatalog`

AWS Configaturan: `tagged-athena-datacatalog` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah katalog data Amazon Athena memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika katalog data tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika katalog data tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke katalog data Athena, lihat Menandai sumber daya Athena di Panduan Pengguna Amazon Athena.

[Athena.3] Kelompok kerja Athena harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Athena::WorkGroup`

AWS Configaturan: `tagged-athena-workgroup` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah workgroup Amazon Athena memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika workgroup tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika workgroup tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke workgroup Athena, lihat Menambahkan dan menghapus tag pada grup kerja individual di Panduan Pengguna Amazon Athena.

[Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Athena::WorkGroup`

AWS Configaturan: athena-workgroup-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup kerja Amazon Athena telah mengaktifkan pencatatan. Kontrol gagal jika workgroup tidak mengaktifkan logging.

Log audit melacak dan memantau aktivitas sistem. Mereka menyediakan catatan peristiwa yang dapat membantu Anda mendeteksi pelanggaran keamanan, menyelidiki insiden, dan mematuhi peraturan. Log audit juga meningkatkan akuntabilitas dan transparansi organisasi Anda secara keseluruhan.

Remediasi

Untuk informasi tentang mengaktifkan pencatatan untuk grup kerja Athena, lihat CloudWatch Mengaktifkan metrik kueri di Athena di Panduan Pengguna Amazon Athena.

Kontrol CSPM Security Hub untukAWS Backup

Kontrol CSPM Security Hub ini mengevaluasi AWS Backup layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Backup::RecoveryPoint`

AWS Configaturan: **`backup-recovery-point-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik AWS Backup pemulihan dienkripsi saat istirahat. Kontrol gagal jika titik pemulihan tidak dienkripsi saat istirahat.

Titik AWS Backup pemulihan mengacu pada salinan atau snapshot data tertentu yang dibuat sebagai bagian dari proses pencadangan. Ini merupakan momen tertentu ketika data dicadangkan dan berfungsi sebagai titik pemulihan jika data asli hilang, rusak, atau tidak dapat diakses. Mengenkripsi titik pemulihan cadangan menambahkan lapisan perlindungan ekstra terhadap akses yang tidak sah. Enkripsi adalah praktik terbaik untuk melindungi kerahasiaan, integritas, dan keamanan data cadangan.

Remediasi

Untuk mengenkripsi titik AWS Backup pemulihan, lihat Enkripsi untuk cadangan AWS Backup di Panduan Pengembang. AWS Backup

[Backup.2]AWS Backuppoin pemulihan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::RecoveryPoint`

AWS Configaturan: `tagged-backup-recoverypoint` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah titik AWS Backup pemulihan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika titik pemulihan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik pemulihan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menyalin tag dari sumber daya pada waktu pembuatan cadangan, lihat Menyalin tag ke cadangan di Panduan AWS BackupPengembang.

Tag tidak disalin pada waktu pembuatan untuk titik parent/composite pemulihan. Untuk menambahkan tag pada titik pemulihan yang ada termasuk titik parent/composite pemulihan, lihat Menambahkan atau menghapus tag pada titik pemulihan yang ada di Panduan AWS Backup Pengembang.

[Backup.3]AWS Backupbrankas harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::BackupVault`

AWS Configaturan: `tagged-backup-backupvault` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Backup vault memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika titik pemulihan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik pemulihan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag keAWS Backupvault

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Masukkan kunci dan nilai untuk tanda tersebut. Pilih Tambahkan tag baru untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.4]AWS Backuprencana laporan harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::ReportPlan`

AWS Configaturan: `tagged-backup-reportplan` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah rencana AWS Backup laporan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika rencana laporan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika rencana laporan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag keAWS Backuprencana laporan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[Backup.5]AWS Backuprencana cadangan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Backup::BackupPlan`

AWS Configaturan: `tagged-backup-backupplan` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah rencana AWS Backup cadangan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika paket cadangan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika paket cadangan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag keAWS Backuprencana cadangan

1. Buka AWS Backup konsol di https://console.aws.amazon.com/backup.
2. Di panel navigasi, pilih Brankas cadangan.
3. Pilih brankas cadangan dari daftar.
4. Di bagian Backup vault tags, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

Kontrol CSPM Security Hub untukAWS Batch

Kontrol CSPM Security Hub ini mengevaluasi AWS Batch layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Batch.1] Antrian pekerjaan batch harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Batch::JobQueue`

AWS Configaturan: batch-job-queue-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratanAWS.	

Kontrol ini memeriksa apakah antrian AWS Batch pekerjaan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika antrian pekerjaan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antrian pekerjaan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke antrean pekerjaan Batch, lihat Menandai sumber daya Anda di Panduan AWS Batch Pengguna.

[Batch.2] Kebijakan penjadwalan Batch harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Batch::SchedulingPolicy`

AWS Configaturan: batch-scheduling-policy-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah kebijakan AWS Batch penjadwalan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika kebijakan penjadwalan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan penjadwalan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan

tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke kebijakan penjadwalan Batch, lihat Menandai sumber daya Anda di Panduan AWS Batch Pengguna.

[Batch.3] Lingkungan komputasi Batch harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Batch::ComputeEnvironment`

AWS Configaturan: batch-compute-environment-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah lingkungan AWS Batch komputasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika lingkungan komputasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika lingkungan komputasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke lingkungan komputasi Batch, lihat Menandai sumber daya Anda di Panduan AWS Batch Pengguna.

[Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Batch::ComputeEnvironment`

AWS Configaturan: batch-managed-compute-env-compute-resources-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah properti sumber daya komputasi di lingkungan AWS Batch komputasi terkelola memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika properti sumber daya komputasi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika properti sumber daya komputasi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan. Kontrol ini tidak mengevaluasi lingkungan komputasi yang tidak dikelola, atau lingkungan terkelola yang menggunakan AWS Fargate sumber daya.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag untuk menghitung sumber daya di lingkungan AWS Batch komputasi terkelola, lihat Menandai sumber daya Anda di AWS BatchPanduan Pengguna.

Kontrol CSPM Security Hub untuk Amazon Bedrock

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Bedrock. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Bedrock.1] Sumber data Amazon Bedrock harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Bedrock::DataSource`

AWS Configaturan: bedrock-data-source-encryption-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sumber data Amazon Bedrock dienkripsi saat istirahat dengan kunci yang dikelola pelanggan. AWS KMS Kontrol gagal jika sumber data tidak dienkripsi dengan kunci KMS yang dikelola pelanggan.

Secara default, Amazon Bedrock mengenkripsi konten sumber data dengan AWS kunci terkelola. Menggunakan kunci KMS yang dikelola pelanggan memberi Anda kontrol penuh atas siklus hidup kunci enkripsi, termasuk rotasi, kebijakan akses, dan audit. AWS CloudTrail Ini membantu memenuhi persyaratan kepatuhan yang mengamanatkan enkripsi yang dikendalikan pelanggan untuk data sensitif yang dicerna ke dalam basis pengetahuan.

Remediasi

Untuk mengenkripsi sumber data Amazon Bedrock Anda dengan kunci KMS yang dikelola pelanggan, lihat Memodifikasi sumber data untuk basis pengetahuan Amazon Bedrock Anda di Panduan Pengguna Amazon Bedrock.

Kontrol CSPM Security Hub untuk Amazon Bedrock AgentCore

AWS Security Hub CSPMKontrol ini mengevaluasi AgentCore layanan dan sumber daya Amazon Bedrock. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::BedrockAgentCore::Runtime`

AWS Configaturan: bedrockagentcore-runtime-private-network-required

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AgentCore runtime Amazon Bedrock dikonfigurasi dengan mode jaringan VPC. Kontrol gagal jika runtime memiliki mode jaringan yang disetel ke PUBLIC.

Menggunakan mode jaringan publik untuk AgentCore runtime Amazon Bedrock mengekspos runtime langsung ke internet, meningkatkan permukaan serangan dan risiko akses tidak sah.

Mengkonfigurasi runtime dengan mode jaringan VPC memastikan bahwa lalu lintas runtime terbatas dalam jaringan pribadi Anda, memungkinkan Anda untuk menerapkan kontrol keamanan tingkat jaringan seperti grup keamanan, ACL jaringan, dan log aliran VPC.

Remediasi

Untuk memulihkan temuan ini, perbarui AgentCore runtime Bedrock yang tidak sesuai dan konfigurasikan dengan mode jaringan VPC. Untuk petunjuknya, lihat Mengonfigurasi AgentCore Runtime Amazon Bedrock dan alat untuk VPC di Panduan Pengembang Amazon Bedrock. AgentCore

[BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::BedrockAgentCore::Gateway`

AWS Configaturan: bedrockagentcore-gateway-authorizer-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon Bedrock AgentCore Gateway memerlukan otorisasi untuk permintaan masuk. Kontrol gagal jika Bedrock AgentCore Gateway tidak memiliki otorisasi masuk yang disiapkan.

Mengkonfigurasi otentikasi di AgentCore gateway Amazon Bedrock memastikan bahwa hanya klien yang berwenang yang dapat mengirim permintaan ke agen AI Anda. Tanpa otorisasi, entitas apa pun yang memiliki akses jaringan ke titik akhir gateway dapat memanggil agen Anda, yang berpotensi menyebabkan akses data yang tidak sah, penyalahgunaan sumber daya, atau biaya tak terduga. Otorisasi masuk memvalidasi pengguna yang mencoba mengakses target melalui gateway Anda. AgentCore

Remediasi

Untuk menyiapkan otorisasi masuk untuk Amazon Bedrock AgentCore Gateway, lihat Menyiapkan otorisasi masuk untuk gateway Anda di Panduan Pengembang Amazon Bedrock. AgentCore

[BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

Persyaratan terkait: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::BedrockAgentCore::Memory`

AWS Configaturan: bedrock-agentcore-memory-encryption-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AgentCore Memori Bedrock Amazon dienkripsi saat istirahat dengan kunci yang dikelola pelanggan. AWS KMS Kontrol gagal jika AgentCore Memori Batuan Dasar tidak dienkripsi dengan kunci KMS yang dikelola pelanggan.

Menggunakan kunci KMS yang dikelola pelanggan untuk enkripsi AgentCore memori Amazon Bedrock memberikan keamanan yang ditingkatkan melalui kunci terkelola layanan default. Kunci KMS yang dikelola pelanggan memberi Anda kontrol penuh atas siklus hidup kunci enkripsi dan kebijakan akses. Selain itu, semua penggunaan kunci enkripsi dapat dicatat dan dipantau AWS CloudTrail untuk auditabilitas.

Remediasi

Untuk mengenkripsi AgentCore Memori Amazon Bedrock Anda dengan kunci KMS yang dikelola pelanggan, lihat Mengenkripsi AgentCore Memori Amazon Bedrock Anda di Panduan Pengembang Amazon Bedrock. AgentCore

[BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

Persyaratan terkait: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan data > Enkripsi data saat istirahat

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::BedrockAgentCore::Gateway`

AWS Configaturan: bedrockagentcore-gateway-encryption-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon Bedrock AgentCore Gateway dienkripsi saat istirahat dengan kunci yang dikelola pelanggan. AWS KMS Kontrol gagal jika Bedrock AgentCore Gateway tidak dienkripsi dengan kunci KMS yang dikelola pelanggan.

Secara default, Amazon Bedrock AgentCore mengenkripsi data gateway dengan AWS kunci terkelola. Menggunakan kunci KMS yang dikelola pelanggan memberi Anda kontrol penuh atas siklus hidup kunci enkripsi, termasuk rotasi, kebijakan akses, dan audit. AWS CloudTrail Ini membantu memenuhi persyaratan kepatuhan yang mengamanatkan enkripsi yang dikendalikan pelanggan untuk beban kerja AI yang sensitif.

Remediasi

Untuk mengenkripsi AgentCore Gateway Bedrock Anda dengan kunci KMS yang dikelola pelanggan, lihat Mengenkripsi AgentCore gateway Anda dengan kunci KMS yang dikelola pelanggan di Panduan Pengembang Amazon Bedrock. AgentCore

[BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::BedrockAgentCore::BrowserCustom`

AWS Configaturan: bedrockagentcore-browsercustom-network-mode-not-public

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah browser AgentCore kustom Amazon Bedrock dikonfigurasi dengan mode jaringan publik. Kontrol gagal jika mode jaringan diatur ke publik.

Menggunakan mode jaringan PUBLIK untuk browser AgentCore kustom Amazon Bedrock mengekspos sesi browser langsung ke internet, meningkatkan permukaan serangan dan risiko akses yang tidak sah. Mengkonfigurasi browser dengan mode jaringan VPC memastikan bahwa lalu lintas browser terbatas dalam jaringan pribadi Anda, memungkinkan Anda untuk menerapkan kontrol keamanan tingkat jaringan seperti grup keamanan, ACL jaringan, dan log aliran VPC.

Remediasi

Untuk memulihkan temuan ini, hapus browser AgentCore kustom Bedrock yang tidak sesuai dan buat ulang dengan mode jaringan VPC. Untuk petunjuknya, lihat Mengonfigurasi AgentCore Runtime Amazon Bedrock dan alat untuk VPC di Panduan Pengembang Amazon Bedrock. AgentCore

[BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::BedrockAgentCore::BrowserCustom`

AWS Configaturan: bedrockagentcore-browsercustom-recording-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah browser AgentCore kustom Amazon Bedrock mengaktifkan perekaman sesi dengan tujuan S3 yang dikonfigurasi. Kontrol gagal jika browser khusus tidak mengaktifkan perekaman atau tidak memiliki lokasi S3 yang dikonfigurasi untuk menyimpan rekaman.

Rekaman sesi untuk browser AgentCore kustom Bedrock memastikan auditabilitas penuh interaksi browser, memungkinkan deteksi akses tidak sah, eksfiltrasi data, atau aktivitas berbahaya selama sesi penjelajahan otomatis.

Remediasi

Untuk petunjuk tentang cara mengaktifkan perekaman sesi browser, lihat Perekaman Sesi dan Putar Ulang di Panduan AgentCore Pengembang Amazon Bedrock.

[BedrockAgentCore.7] Interpreter kode AgentCore kustom batuan dasar harus menggunakan konfigurasi jaringan pribadi

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::BedrockAgentCore::CodeInterpreterCustom`

AWS Configaturan: bedrockagentcore-codeinterpreter-networkmode-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penerjemah kode AgentCore kustom Amazon Bedrock dikonfigurasi dengan mode jaringan pribadi. Kontrol gagal jika mode jaringan diatur ke `PUBLIC` atau`SANDBOX`.

Mengkonfigurasi interpreter kode AgentCore kustom Bedrock dengan mode jaringan pribadi memastikan bahwa lingkungan eksekusi kode terisolasi dalam VPC Anda. Mode jaringan publik atau kotak pasir mengekspos penerjemah kode ke internet, meningkatkan risiko akses tidak sah dan eksfiltrasi data. Menggunakan mode jaringan pribadi membatasi akses jaringan dan membantu melindungi data sensitif yang diproses selama interpretasi kode.

Remediasi

Untuk memulihkan temuan ini, hapus interpreter kode AgentCore kustom Bedrock yang tidak sesuai dan buat ulang dengan mode jaringan VPC. Untuk petunjuknya, lihat Mengonfigurasi akses VPC untuk runtime dan alat di Panduan Pengembang Amazon AgentCore Bedrock.

Kontrol CSPM Security Hub untukAWS Certificate Manager

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya AWS Certificate Manager (ACM). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu

Persyaratan terkait: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16), NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ACM::Certificate`

AWS Configaturan: acm-certificate-expiration-check

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`daysToExpiration`	Jumlah hari di mana sertifikat ACM harus diperpanjang	Bilangan Bulat	`14` untuk `365`	`30`

Kontrol ini memeriksa apakah sertifikat AWS Certificate Manager (ACM) diperbarui dalam jangka waktu yang ditentukan. Ini memeriksa sertifikat impor dan sertifikat yang disediakan oleh ACM. Kontrol gagal jika sertifikat tidak diperpanjang dalam jangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode perpanjangan, Security Hub CSPM menggunakan nilai default 30 hari.

ACM dapat secara otomatis memperbarui sertifikat yang menggunakan validasi DNS. Untuk sertifikat yang menggunakan validasi email, Anda harus menanggapi email validasi domain. ACM tidak secara otomatis memperbarui sertifikat yang Anda impor. Anda harus memperbarui sertifikat yang diimpor secara manual.

Remediasi

ACM menyediakan perpanjangan terkelola untuk SSL/TLS sertifikat yang dikeluarkan oleh Amazon. Ini berarti bahwa ACM memperbarui sertifikat Anda secara otomatis (jika Anda menggunakan validasi DNS), atau mengirimi Anda pemberitahuan email ketika kedaluwarsa sertifikat mendekati. Layanan ini disediakan untuk sertifikat ACM publik dan swasta.

Untuk domain yang divalidasi melalui email

> Ketika sertifikat 45 hari dari kedaluwarsa, ACM mengirimkan email kepada pemilik domain untuk setiap nama domain. Untuk memvalidasi domain dan menyelesaikan perpanjangan, Anda harus menanggapi pemberitahuan email.
>
> Untuk informasi selengkapnya, lihat Perpanjangan domain yang divalidasi melalui email di Panduan Pengguna. AWS Certificate Manager

Untuk domain yang divalidasi oleh DNS

ACM secara otomatis memperbarui sertifikat yang menggunakan validasi DNS. 60 hari sebelum kedaluwarsa, ACM memverifikasi bahwa sertifikat dapat diperpanjang.

Jika tidak dapat memvalidasi nama domain, maka ACM mengirimkan pemberitahuan bahwa validasi manual diperlukan. Ini mengirimkan pemberitahuan ini 45 hari, 30 hari, 7 hari, dan 1 hari sebelum kedaluwarsa.

Untuk informasi selengkapnya, lihat Perpanjangan domain yang divalidasi oleh DNS di Panduan Pengguna. AWS Certificate Manager

[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

Persyaratan terkait: PCI DSS v4.0. 1/4.2.1

Kategori: Identifikasi > Persediaan > Layanan inventaris

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ACM::Certificate`

AWS Configaturan: acm-certificate-rsa-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sertifikat RSA dikelola dengan AWS Certificate Manager menggunakan panjang kunci minimal 2.048 bit. Kontrol gagal jika panjang kunci lebih kecil dari 2.048 bit.

Kekuatan enkripsi berkorelasi langsung dengan ukuran kunci. Kami merekomendasikan panjang kunci setidaknya 2.048 bit untuk melindungi AWS sumber daya Anda karena daya komputasi menjadi lebih murah dan server menjadi lebih maju.

Remediasi

Panjang kunci minimum untuk sertifikat RSA yang dikeluarkan oleh ACM sudah 2.048 bit. Untuk petunjuk tentang menerbitkan sertifikat RSA baru dengan ACM, lihat Menerbitkan dan mengelola sertifikat di Panduan Pengguna. AWS Certificate Manager

Meskipun ACM memungkinkan Anda untuk mengimpor sertifikat dengan panjang kunci yang lebih pendek, Anda harus menggunakan kunci minimal 2.048 bit untuk melewati kontrol ini. Anda

tidak dapat mengubah panjang kunci setelah mengimpor sertifikat. Sebagai gantinya, Anda harus menghapus sertifikat dengan panjang kunci lebih kecil dari 2.048 bit. Untuk informasi selengkapnya tentang mengimpor sertifikat ke ACM, lihat Prasyarat untuk mengimpor sertifikat di Panduan Pengguna. AWS Certificate Manager

[ACM.3] Sertifikat ACM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ACM::Certificate`

AWS Configaturan: `tagged-acm-certificate` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah sertifikat AWS Certificate Manager (ACM) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber

daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke sertifikat ACM, lihat Menandai AWS Certificate Manager sertifikat di AWS Certificate ManagerPanduan Pengguna.

Kontrol CSPM Security Hub untukCloudFormation

Kontrol CSPM Security Hub ini mengevaluasi AWS CloudFormation layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudFormation.1] CloudFormation tumpukan harus diintegrasikan dengan Simple Notification Service (SNS)

> **Important**
>
> Security Hub CSPM menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Log perubahan untuk kontrol CSPM Security Hub.

Persyaratan terkait: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFormation::Stack`

AWS Configaturan: **`cloudformation-stack-notification-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemberitahuan Amazon Simple Notification Service terintegrasi dengan CloudFormation tumpukan. Kontrol gagal untuk CloudFormation tumpukan jika tidak ada pemberitahuan SNS yang terkait dengannya.

Mengonfigurasi notifikasi SNS dengan CloudFormation tumpukan Anda membantu segera memberi tahu pemangku kepentingan tentang peristiwa atau perubahan apa pun yang terjadi dengan tumpukan.

Remediasi

Untuk mengintegrasikan CloudFormation tumpukan dan topik SNS, lihat Memperbarui tumpukan secara langsung di AWS CloudFormationPanduan Pengguna.

[CloudFormation.2] CloudFormation tumpukan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFormation::Stack`

AWS Configaturan: `tagged-cloudformation-stack` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratanAWS.	

Kontrol ini memeriksa apakah AWS CloudFormation tumpukan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika tumpukan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tumpukan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CloudFormation tumpukan, lihat CreateStackdi Referensi AWS CloudFormation API.

[CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFormation::Stack`

AWS Configaturan: cloudformation-termination-protection-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS CloudFormation tumpukan memiliki perlindungan terminasi yang diaktifkan. Kontrol gagal jika perlindungan terminasi tidak diaktifkan pada CloudFormation tumpukan.

CloudFormation membantu mengelola sumber daya terkait sebagai satu unit yang disebut Stack. Anda dapat mencegah tumpukan tidak sengaja dihapus dengan mengaktifkan perlindungan terminasi pada tumpukan. Jika pengguna mencoba untuk menghapus tumpukan dengan perlindungan terminasi diaktifkan, penghapusan gagal dan tumpukan, termasuk statusnya, tetap tidak berubah. Anda dapat mengatur perlindungan terminasi pada tumpukan dengan status apa pun kecuali `DELETE_IN_PROGRESS` atau`DELETE_COMPLETE`.

> **Note**
>
> Mengaktifkan atau menonaktifkan perlindungan terminasi pada tumpukan meneruskan pilihan yang sama ke tumpukan bersarang milik tumpukan itu juga. Anda tidak dapat mengaktifkan atau menonaktifkan perlindungan terminasi secara langsung di tumpukan nest. Anda tidak dapat langsung menghapus tumpukan bersarang milik tumpukan yang memiliki perlindungan terminasi diaktifkan. Jika NESTED ditampilkan di sebelah nama tumpukan, tumpukan adalah tumpukan nest. Anda hanya dapat mengubah perlindungan terminasi pada tumpukan akar yang dimiliki tumpukan nest.

Remediasi

Untuk mengaktifkan perlindungan penghentian pada CloudFormation tumpukan, lihat Melindungi CloudFormation tumpukan agar tidak dihapus di Panduan AWS CloudFormation Pengguna.

[CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait

Kategori: Deteksi > Manajemen akses aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFormation::Stack`

AWS Configaturan: cloudformation-stack-service-role-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS CloudFormation tumpukan memiliki peran layanan yang terkait dengannya. Kontrol gagal untuk CloudFormation tumpukan jika tidak ada peran layanan yang terkait dengannya.

Service-managed StackSets menggunakan peran eksekusi melalui integrasi akses terpercaya AWS Organizations. Kontrol juga menghasilkan temuan GAGAL untuk AWS CloudFormation tumpukan yang dibuat oleh service-managed StackSets karena tidak ada peran layanan yang terkait dengannya. Karena cara StackSets autentikasi yang dikelola layanan, `roleARN` bidang tidak dapat diisi untuk tumpukan ini.

Menggunakan peran layanan dengan CloudFormation tumpukan membantu menerapkan akses hak istimewa paling sedikit dengan memisahkan izin antara pengguna yang creates/updates menumpuk dan izin yang diperlukan oleh sumber daya. CloudFormation create/update Ini mengurangi risiko eskalasi hak istimewa dan membantu menjaga batas-batas keamanan antara peran operasional yang berbeda.

> **Note**
>
> Penghapusan peran layanan yang melekat pada tumpukan setelah tumpukan dibuat tidak dapat dilakukan. Pengguna lain yang memiliki izin untuk melakukan operasi pada tumpukan ini dapat menggunakan peran ini, terlepas dari apakah pengguna tersebut memiliki `iam:PassRole` izin atau tidak. Jika peran tersebut mencakup izin yang seharusnya tidak dimiliki pengguna, Anda dapat secara tidak sengaja meningkatkan izin pengguna. Pastikan peran memberikan keistimewaan paling rendah.

Remediasi

Untuk mengaitkan peran layanan dengan CloudFormation tumpukan, lihat peran CloudFormation layanan di Panduan AWS CloudFormation Pengguna.

Kontrol CSPM Hub Keamanan untuk Amazon CloudFront

AWS Security Hub CSPM Kontrol ini mengevaluasi CloudFront layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), PCI DSS v4.0. 1/2.2.6

Kategori: L indungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-default-root-object-configured

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dengan asal S3 dikonfigurasi untuk mengembalikan objek tertentu yang merupakan objek root default. Kontrol gagal jika CloudFront distribusi menggunakan asal S3 dan tidak memiliki objek root default yang dikonfigurasi. Kontrol ini tidak berlaku untuk CloudFront distribusi yang menggunakan asal khusus.

Pengguna terkadang meminta URL root distribusi alih-alih objek dalam distribusi. Ketika ini terjadi, menentukan objek root default dapat membantu Anda menghindari mengekspos konten distribusi web Anda.

Remediasi

Untuk mengonfigurasi objek root default untuk CloudFront distribusi, lihat Cara menentukan objek root default di Panduan CloudFront Pengembang Amazon.

[CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-viewer-policy-https

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon mengharuskan pemirsa menggunakan HTTPS secara langsung atau apakah itu menggunakan pengalihan. Kontrol gagal jika `ViewerProtocolPolicy` disetel ke `allow-all` untuk `defaultCacheBehavior` atau untuk`cacheBehaviors`.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan serangan person-in-the-middle atau serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang boleh diizinkan. Mengenkripsi data dalam transit dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS.

Remediasi

Untuk mengenkripsi CloudFront distribusi yang sedang transit, lihat Mem butuhkan HTTPS untuk komunikasi antar pemirsa dan CloudFront di Panduan CloudFront Pengembang Amazon.

[CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 SC-36,, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-origin-failover-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi dengan grup asal yang memiliki dua atau lebih asal.

CloudFront failover asal dapat meningkatkan ketersediaan. Failover asal secara otomatis mengalihkan lalu lintas ke asal sekunder jika asal utama tidak tersedia atau jika mengembalikan kode status respons HTTP tertentu.

Remediasi

Untuk mengonfigurasi failover asal untuk CloudFront distribusi, lihat Membuat grup asal di Panduan CloudFront Pengembang Amazon.

Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-accesslogs-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging akses server diaktifkan pada CloudFront distribusi. Kontrol gagal jika logging akses tidak diaktifkan untuk distribusi. Kontrol ini hanya mengevaluasi apakah pencatatan standar (lama) diaktifkan untuk distribusi.

CloudFront log akses memberikan informasi terperinci tentang setiap permintaan pengguna yang CloudFront diterima. Setiap log berisi informasi seperti tanggal dan waktu permintaan diterima, alamat IP penampil yang membuat permintaan, sumber permintaan, dan nomor port permintaan dari penampil. Log ini berguna untuk aplikasi seperti audit keamanan dan akses dan investigasi forensik. Untuk informasi selengkapnya tentang menganalisis log akses, lihat Kueri CloudFront log Amazon di Panduan Pengguna Amazon Athena.

Remediasi

Untuk mengonfigurasi pencatatan standar (lama) untuk CloudFront distribusi, lihat Meng onfigurasi pencatatan standar (lama) di Panduan CloudFront Pengembang Amazon.

[CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), PCI DSS v4.0. 1/6.4.2

Kategori: Melindungi > Layanan perlindungan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-associated-with-waf

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi dikaitkan dengan ACL AWS WAF Klasik atau AWS WAF web. Kontrol gagal jika distribusi tidak terkait dengan ACL web.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan API dari serangan. Ini memungkinkan Anda untuk mengonfigurasi seperangkat aturan, yang disebut daftar kontrol akses web (web ACL), yang memungkinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tentukan. Pastikan CloudFront distribusi Anda dikaitkan dengan ACL AWS WAF web untuk membantu melindunginya dari serangan berbahaya.

Remediasi

Untuk mengait AWS WAF kan ACL web dengan CloudFront distribusi, lihat Menggunakan AWS WAF untuk mengontrol akses ke konten Anda di Panduan CloudFront Pengembang Amazon.

[CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-custom-ssl-certificate

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi menggunakan SSL/TLS sertifikat default yang CloudFront disediakan. Kontrol ini lolos jika CloudFront distribusi menggunakan SSL/TLS sertifikat kustom. Kontrol ini gagal jika CloudFront distribusi menggunakan SSL/TLS sertifikat default.

Kustom SSL/TLS memungkinkan pengguna mengakses konten dengan menggunakan nama domain alternatif. Anda dapat menyimpan sertifikat kustom di AWS Certificate Manager (disarankan), atau di IAM.

Remediasi

Untuk menambahkan nama domain alternatif untuk CloudFront distribusi menggunakan SSL/TLS sertifikat khusus, lihat Men ambahkan nama domain alternatif di Panduan CloudFront Pengembang Amazon.

[CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-sni-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menggunakan SSL/TLS sertifikat khusus dan dikonfigurasi untuk menggunakan SNI untuk melayani permintaan HTTPS. Kontrol ini gagal jika SSL/TLS sertifikat kustom dikaitkan tetapi metode SSL/TLS dukungannya adalah alamat IP khusus. Kontrol juga gagal jika distribusi menggunakan CloudFront SSL/TLS sertifikat default.

Indikasi Nama Server (Ser Server Name Indication atau SNI) adalah ekstensi untuk protokol TLS yang didukung oleh browser dan klien yang dirilis setelah tahun 2010. Jika Anda mengonfigurasi CloudFront untuk melayani permintaan HTTPS menggunakan SNI, CloudFront kaitkan nama domain alternatif Anda dengan alamat IP untuk setiap lokasi tepi. Saat penampil mengirimkan permintaan HTTPS untuk konten Anda, DNS mengirimkan permintaan ke alamat IP untuk lokasi tepi yang benar. Alamat IP untuk nama domain Anda ditentukan selama negosiasi SSL/TLS jabat tangan; alamat IP tidak didedikasikan untuk distribusi Anda.

Remediasi

Untuk mengonfigurasi CloudFront distribusi agar menggunakan SNI untuk melayani permintaan HTTPS, lihat Menggunakan SNI untuk Melayani Permintaan HTTPS (berfungsi untuk Sebagian besar Klien) di Panduan Peng CloudFront embang. Untuk informasi tentang sertifikat SSL khusus, lihat Per syaratan untuk menggunakan SSL/TLS sertifikat dengan CloudFront.

[CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-traffic-to-origin-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon mengenkripsi lalu lintas ke sumber khusus. Kontrol ini gagal untuk CloudFront distribusi yang kebijakan protokol asalnya mengizinkan 'http-only'. Kontrol ini juga gagal jika kebijakan protokol asal distribusi adalah 'match-viewer' sedangkan kebijakan protokol penampil adalah 'allow-all'.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyadapan atau manipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang boleh diizinkan.

Remediasi

Untuk memperbarui Kebijakan Protokol Asal agar memerlukan enkripsi untuk CloudFront koneksi, lihat M emerlukan HTTPS untuk komunikasi antara CloudFront dan asal kustom Anda di Panduan CloudFront Pengembang Amazon.

[CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-no-deprecated-ssl-protocols

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menggunakan protokol SSL yang tidak digunakan lagi untuk komunikasi HTTPS antara lokasi CloudFront tepi dan asal kustom Anda. Kontrol ini gagal jika CloudFront distribusi memiliki `CustomOriginConfig` where `OriginSslProtocols` include`SSLv3`.

Pada tahun 2015, Satuan Tugas Rekayasa Internet (IETF) secara resmi mengumumkan bahwa SSL 3.0 harus ditinggalkan karena protokol tidak cukup aman. Disarankan agar Anda menggunakan TLSv1.2 atau yang lebih baru untuk komunikasi HTTPS ke sumber kustom Anda.

Remediasi

Untuk memperbarui Protokol SSL Asal untuk CloudFront distribusi, lihat M emerlukan HTTPS untuk komunikasi antara CloudFront dan asal kustom Anda di Panduan CloudFront Pengembang Amazon.

[CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada

Persyaratan terkait: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), PCI DSS v4.0. 1/2.2.6

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-s3-origin-non-existent-bucket

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon menunjuk ke asal Amazon S3 yang tidak ada. Kontrol gagal untuk CloudFront distribusi jika asal dikonfigurasi untuk menunjuk ke bucket yang tidak ada. Kontrol ini hanya berlaku untuk CloudFront distribusi di mana bucket S3 tanpa hosting situs web statis adalah asal S3.

Ketika CloudFront distribusi di akun Anda dikonfigurasi untuk menunjuk ke bucket yang tidak ada, pihak ketiga jahat dapat membuat bucket yang direferensikan dan menyajikan konten mereka sendiri melalui distribusi Anda. Sebaiknya periksa semua asal terlepas dari perilaku perutean untuk memastikan bahwa distribusi Anda menunjuk ke asal yang sesuai.

Remediasi

Untuk mengubah CloudFront distribusi agar mengarah ke asal baru, lihat Memper barui distribusi di Panduan CloudFront Pengembang Amazon.

[CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

Kategori: L indungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-s3-origin-access-control-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dengan asal Amazon S3 memiliki kontrol akses asal (OAC) yang dikonfigurasi. Kontrol gagal jika OAC tidak dikonfigurasi untuk CloudFront distribusi.

Saat menggunakan bucket S3 sebagai sumber untuk CloudFront distribusi Anda, Anda dapat mengaktifkan OAC. Ini memungkinkan akses ke konten dalam bucket hanya melalui CloudFront distribusi yang ditentukan, dan melarang akses langsung dari bucket atau distribusi lain. Meskipun CloudFront mendukung Origin Access Identity (OAI), OAC menawarkan fungsionalitas tambahan, dan distribusi menggunakan OAI dapat bermigrasi ke OAC. Meskipun OAI menyediakan cara aman untuk mengakses asal S3, ia memiliki keterbatasan, seperti kurangnya dukungan untuk konfigurasi kebijakan terperinci dan untuk HTTP/HTTPS permintaan yang menggunakan metode POST Wilayah AWS yang memerlukan Sig AWS nature Version 4 (SIGv4). OAI juga tidak mendukung enkripsi dengan AWS Key Management Service. OAC didasarkan pada praktik AWS terbaik menggunakan prinsip-prinsip layanan IAM untuk mengotentikasi dengan asal S3.

Remediasi

Untuk mengonfigurasi OAC untuk CloudFront distribusi dengan asal S3, lihat Membatasi akses ke sumber Amazon S3 di Panduan CloudFront Pengembang Amazon.

[CloudFront.14] CloudFront distribusi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: `tagged-cloudfront-distribution` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah CloudFront distribusi Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika distribusi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika distribusi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Menandai juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CloudFront distribusi, lihat Men andai CloudFront distribusi Amazon di Panduan CloudFront Pengembang Amazon.

[CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-ssl-policy-check

Jenis jadwal: Perubahan dipicu

Parameter: `securityPolicies`: `TLSv1.2_2021,TLSv1.2_2025,TLSv1.3_2025` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk menggunakan kebijakan keamanan TLS yang direkomendasikan. Kontrol gagal jika CloudFront distribusi tidak dikonfigurasi untuk menggunakan kebijakan keamanan TLS yang direkomendasikan.

Jika Anda mengonfigurasi CloudFront distribusi Amazon untuk mengharuskan pemirsa menggunakan HTTPS untuk mengakses konten, Anda harus memilih kebijakan keamanan dan menentukan versi SSL/TLS protokol minimum yang akan digunakan. Ini menentukan versi protokol mana yang CloudFront digunakan untuk berkomunikasi dengan pemirsa, dan sandi yang digunakan untuk CloudFront mengenkripsi komunikasi. Sebaiknya gunakan kebijakan keamanan terbaru yang CloudFront disediakan. Ini memastikan bahwa CloudFront menggunakan suite sandi terbaru untuk mengenkripsi data yang sedang transit antara penampil dan CloudFront distribusi.

> **Note**
>
> Kontrol ini menghasilkan temuan hanya untuk CloudFront distribusi yang dikonfigurasi untuk menggunakan sertifikat SSL khusus dan tidak dikonfigurasi untuk mendukung klien lama.

Remediasi

Untuk informasi tentang mengonfigurasi kebijakan keamanan untuk CloudFront distribusi, lihat Memperbarui distribusi di Panduan CloudFront Pengembang Amazon. Saat Anda mengonfigurasi kebijakan keamanan untuk distribusi, pilih kebijakan keamanan terbaru.

Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal

Kategori: Melindungi > Manajemen akses aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-origin-lambda-url-oac-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dengan URL AWS Lambda fungsi sebagai sumber mengaktifkan kontrol akses asal (OAC). Kontrol gagal jika CloudFront distribusi memiliki URL fungsi Lambda sebagai asal dan OAC tidak diaktifkan.

URL AWS Lambda fungsi adalah titik akhir HTTPS khusus untuk fungsi Lambda. Jika URL fungsi Lambda adalah asal untuk CloudFront distribusi, URL fungsi harus dapat diakses publik. Oleh karena itu, sebagai praktik terbaik keamanan, Anda harus membuat OAC dan menambahkannya ke URL fungsi Lambda dalam distribusi. OAC menggunakan prinsipal layanan IAM untuk mengotentikasi permintaan antara CloudFront dan URL fungsi. Ini juga mendukung penggunaan kebijakan berbasis sumber daya untuk mengizinkan pemanggilan fungsi hanya jika permintaan atas nama CloudFront distribusi yang ditentukan dalam kebijakan.

Remediasi

Untuk informasi tentang mengonfigurasi OAC untuk CloudFront distribusi Amazon yang menggunakan URL fungsi Lambda sebagai sumber, lihat Mem batasi akses ke sumber URL AWS Lambda fungsi di Panduan CloudFront Pengembang Amazon.

Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani

Kategori: Melindungi > Manajemen akses aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudFront::Distribution`

AWS Config aturan: cloudfront-distribution-key-group-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudFront distribusi Amazon dikonfigurasi untuk menggunakan grup kunci tepercaya untuk URL yang ditandatangani atau otentikasi cookie yang ditandatangani. Kontrol gagal jika CloudFront distribusi menggunakan penandatangan tepercaya, atau jika distribusi tidak memiliki otentikasi yang dikonfigurasi.

Menggunakan tanda tangan atau cookie yang ditandatangani, Anda perlu signer. Penandatangan adalah grup kunci tepercaya yang Anda buat CloudFront, atau AWS akun yang berisi pasangan CloudFront kunci. Sebaiknya gunakan grup kunci tepercaya karena dengan grup CloudFront kunci, Anda tidak perlu menggunakan pengguna root AWS akun untuk mengelola kunci publik untuk URL yang CloudFront ditandatangani dan cookie yang ditandatangani.

> **Note**
>
> Kontrol ini tidak mengevaluasi CloudFront distribusi (`connectionMode=tenant-only`) multi-tenant.

Remediasi

Untuk informasi tentang menggunakan grup kunci tepercaya dengan URL dan cookie yang ditandatangani, lihat Menggunakan grup kunci tepercaya di Panduan CloudFront Pengembang Amazon.

Kontrol CSPM Security Hub untukAWS CloudTrail

AWS Security Hub CSPMKontrol ini mengevaluasi AWS CloudTrail layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/3.1, Tolok Ukur Yayasan AWS CIS v1.2. 0/2.1, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.1, Tolok Ukur Yayasan AWS CIS v3.0. 0/3.1, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), (4), NIST.800-53.r5 AU-6 (1),, NIST.800-53.r5 AU-14 (9) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (8), NIST.800-53.r5 SI-3 (20), NIST.800-53.r5 SI-4 (8), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SA-8 (22)

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: multi-region-cloudtrail-enabled

Jenis jadwal: Periodik

Parameter:

- `readWriteType`: `ALL` (tidak dapat disesuaikan)

  `includeManagementEvents`: `true` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah ada setidaknya satu AWS CloudTrail jejak Multi-wilayah yang menangkap peristiwa manajemen baca dan tulis. Kontrol gagal jika CloudTrail dinonaktifkan atau jika tidak ada setidaknya satu CloudTrail jejak yang menangkap peristiwa manajemen baca dan tulis.

AWS CloudTrailmerekam panggilan AWS API untuk akun Anda dan mengirimkan file log kepada Anda. Informasi yang direkam mencakup informasi berikut:

- Identitas pemanggil API
- Waktu panggilan API
- Alamat IP sumber pemanggil API
- Permintaan parameter
- Elemen respons yang dikembalikan oleh Layanan AWS

CloudTrail menyediakan riwayat panggilan AWS API untuk akun, termasuk panggilan API yang dibuat dariKonsol Manajemen AWS, AWS SDK, alat baris perintah. Riwayat ini juga mencakup panggilan API dari tingkat yang lebih tinggi Layanan AWS seperti. AWS CloudFormation

Riwayat panggilan AWS API yang dihasilkan CloudTrail memungkinkan analisis keamanan, pelacakan perubahan sumber daya, dan audit kepatuhan. Multi-Region jalan setapak juga memberikan manfaat sebagai berikut.

- Jejak multi-wilayah membantu mendeteksi aktivitas tak terduga yang terjadi di Wilayah yang tidak digunakan.
- Jejak multi-wilayah memastikan bahwa pencatatan peristiwa layanan global diaktifkan untuk jejak secara default. Pencatatan peristiwa layanan global mencatat peristiwa yang dihasilkan oleh layanan AWS global.
- Untuk jejak Multi-wilayah, acara manajemen untuk semua operasi baca dan tulis memastikan bahwa operasi manajemen CloudTrail catatan pada semua sumber daya dalam fileAkun AWS.

Secara default, CloudTrail jalur yang dibuat menggunakan jalur Multi-wilayah. Konsol Manajemen AWS

Remediasi

Untuk membuat jejak Multi-wilayah baru CloudTrail, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna. Gunakan nilai berikut:

Bidang	Nilai
Pengaturan tambahan, Validasi file log	Diaktifkan
Pilih peristiwa log, Kejadian manajemen, aktivitas API	Baca dan Tulis. Kosongkan kotak centang untuk pengecualian.

Untuk memperbarui jejak yang ada, lihat Memperbarui jejak di Panduan AWS CloudTrail Pengguna. Di acara Manajemen, untuk aktivitas API, pilih Baca dan Tulis.

[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/3.5, Tolok Ukur Yayasan AWS CIS v1.2. 0/2.7, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.7, Tolok Ukur Yayasan AWS CIS v3.0. 0/3.5,

NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (1) NIST.800-53.r5 SC-28, (10), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.3.8, PCI DSS v3.2. 1/3.4, PCI DSS v4.0. 1/10.3.2

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Configaturan: cloud-trail-encryption-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudTrail dikonfigurasi untuk menggunakan enkripsi server-side encryption (SSE). AWS KMS key Kontrol gagal jika `KmsKeyId` tidak ditentukan.

Untuk lapisan keamanan tambahan untuk file CloudTrail log sensitif Anda, Anda harus menggunakan enkripsi sisi server dengan AWS KMS keys (SSE-KMS) untuk file CloudTrail log Anda untuk enkripsi saat istirahat. Perhatikan bahwa secara default, file log yang dikirimkan CloudTrail ke bucket Anda dienkripsi oleh enkripsi sisi server Amazon dengan kunci enkripsi Amazon S3-managed (). SSE-S3

Remediasi

Untuk mengaktifkan SSE-KMS enkripsi untuk file CloudTrail log, lihat Memperbarui jejak untuk menggunakan kunci KMS di Panduan AWS CloudTrail Pengguna.

[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan

Persyaratan terkait: NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/10.1, PCI DSS v3.2. 1/10.2.1, PCI DSS v3.2. 1/10.2.2, PCI DSS v3.2. 1/10.2.3, PCI DSS v3.2. 1/10.2.4, PCI DSS v3.2. 1/10.2.5, PCI DSS v3.2. 1/10.2.6, PCI DSS v3.2. 1/10.2.7, PCI DSS v3.2. 1/10.3.1, PCI DSS v3.2. 1/10.3.2, PCI DSS v3.2. 1/10.3.3, PCI DSS v3.2. 1/10.3.4, PCI DSS v3.2. 1/10.3.5, PCI DSS v3.2. 1/10.3.6, PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: cloudtrail-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS CloudTrail jejak diaktifkan di AndaAkun AWS. Kontrol gagal jika akun Anda tidak memiliki setidaknya satu CloudTrail jejak yang diaktifkan.

Namun, beberapa AWS layanan tidak mengaktifkan pencatatan semua API dan peristiwa. Anda harus menerapkan jejak audit tambahan selain CloudTrail dan meninjau dokumentasi untuk setiap layanan di Layanan dan Integrasi yang CloudTrail Didukung.

Remediasi

Untuk memulai CloudTrail dan membuat jejak, lihat AWS CloudTrailtutorial Memulai dengan di Panduan AWS CloudTrail Pengguna.

[CloudTrail.4] validasi file CloudTrail log harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/3.2, Tolok Ukur Yayasan AWS CIS v1.2. 0/2.2, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.2, Tolok Ukur Yayasan AWS CIS v3.0. 0/3.2,, NIST.800-53.r5 AU-9 NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (1), (3), NIST.800-53.r5 SI-7 NIST.800-53.r5 SI-7 (7), NIST.800-171.r2 3.3.8, PCI DSS v3.2. 1/10.5.2, PCI DSS v3.2. 1/10.5.5, PCI DSS v4.0. 1/10.3.2

Kategori: Perlindungan data > Integritas data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Configaturan: cloud-trail-log-file-validation-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah validasi integritas file log diaktifkan pada CloudTrail jejak.

CloudTrail validasi file log membuat file digest yang ditandatangani secara digital yang berisi hash dari setiap log yang menulis ke CloudTrail Amazon S3. Anda dapat menggunakan file intisari ini untuk menentukan apakah file log diubah, dihapus, atau tidak diubah setelah CloudTrail mengirimkan log.

Security Hub CSPM merekomendasikan agar Anda mengaktifkan validasi file di semua jalur. Validasi file log memberikan pemeriksaan integritas tambahan CloudTrail log.

Remediasi

Untuk mengaktifkan validasi file CloudTrail log, lihat Mengaktifkan validasi integritas file log CloudTrail di Panduan Pengguna. AWS CloudTrail

[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/3.4, PCI DSS v3.2. 1/10.5.3, Tolok Ukur Yayasan CIS AWS v1.2. 0/2.4, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.4, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-7 (1),, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Configaturan: cloud-trail-cloud-watch-logs-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudTrail jejak dikonfigurasi untuk mengirim log ke CloudWatch Log. Kontrol gagal jika `CloudWatchLogsLogGroupArn` properti jejak kosong.

CloudTrail merekam panggilan AWS API yang dibuat di akun tertentu. Informasi yang direkam meliputi yang berikut:

- Identitas pemanggil API

- Waktu panggilan API
- Alamat IP sumber pemanggil API
- Parameter permintaan
- Elemen respons yang dikembalikan oleh Layanan AWS

CloudTrail menggunakan Amazon S3 untuk penyimpanan dan pengiriman file log. Anda dapat menangkap CloudTrail log dalam bucket S3 tertentu untuk analisis jangka panjang. Untuk melakukan analisis real-time, Anda dapat mengonfigurasi CloudTrail untuk mengirim log ke CloudWatch Log.

Untuk jejak yang diaktifkan di semua Wilayah dalam akun, CloudTrail kirimkan file log dari semua Wilayah tersebut ke grup CloudWatch log Log.

Security Hub CSPM merekomendasikan agar Anda mengirim CloudTrail log ke CloudWatch Log. Perhatikan bahwa rekomendasi ini dimaksudkan untuk memastikan bahwa aktivitas akun ditangkap, dipantau, dan diwaspadai dengan tepat. Anda dapat menggunakan CloudWatch Log untuk mengatur ini dengan AndaLayanan AWS. Rekomendasi ini tidak menghalangi penggunaan solusi yang berbeda.

Mengirim CloudTrail CloudWatch log ke Log memfasilitasi pencatatan aktivitas real-time dan historis berdasarkan pengguna, API, sumber daya, dan alamat IP. Anda dapat menggunakan pendekatan ini untuk membuat alarm dan pemberitahuan untuk aktivitas akun anomali atau sensitivitas.

Remediasi

Untuk mengintegrasikan CloudTrail dengan CloudWatch Log, lihat Mengirim peristiwa ke CloudWatch Log di Panduan AWS CloudTrail Pengguna.

[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/2.3, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.3, PCI DSS v4.0. 1/1.4.4

Kategori: Identifikasi > Logging

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::Bucket`

AWS Configaturan: Tidak ada (aturan CSPM Security Hub kustom)

Jenis jadwal: Berkala dan perubahan dipicu

Parameter: Tidak ada

CloudTrail mencatat catatan setiap panggilan API yang dilakukan di akun Anda. File log ini disimpan dalam ember S3. CIS merekomendasikan agar kebijakan bucket S3, atau daftar kontrol akses (ACL), diterapkan pada bucket S3 yang mencatat untuk mencegah akses publik ke CloudTrail log. CloudTrail Mengizinkan akses publik ke konten CloudTrail log dapat membantu musuh dalam mengidentifikasi kelemahan dalam penggunaan atau konfigurasi akun yang terpengaruh.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM terlebih dahulu menggunakan logika kustom untuk mencari bucket S3 tempat CloudTrail log Anda disimpan. Kemudian menggunakan aturan AWS Config terkelola untuk memeriksa apakah bucket dapat diakses publik.

Jika Anda menggabungkan log Anda ke dalam satu bucket S3 terpusat, maka Security Hub CSPM hanya menjalankan pemeriksaan terhadap akun dan Wilayah tempat bucket S3 terpusat berada. Untuk akun dan Wilayah lain, status kontrolnya adalah Tidak ada data.

Jika bucket dapat diakses publik, cek akan menghasilkan temuan yang gagal.

Remediasi

Untuk memblokir akses publik ke bucket CloudTrail S3, lihat Mengonfigurasi blokir setelan akses publik untuk bucket S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Pilih keempat Pengaturan Akses Publik Blok Amazon S3.

[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/2.6, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.6, Tolok Ukur Yayasan AWS CIS v3.0. 0/3.4, PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Configaturan: Tidak ada (aturan CSPM Security Hub kustom)

Jenis jadwal: Periodik

Parameter: Tidak ada

Pencatatan akses bucket S3 menghasilkan log yang berisi catatan akses untuk setiap permintaan yang dibuat ke bucket S3 Anda. Catatan log akses berisi rincian tentang permintaan, seperti jenis permintaan, sumber daya yang ditentukan dalam permintaan berfungsi, dan waktu dan tanggal permintaan diproses.

CIS menyarankan agar Anda mengaktifkan pencatatan akses bucket pada bucket CloudTrail S3.

Dengan mengaktifkan pencatatan bucket S3 pada bucket S3 target, Anda dapat menangkap semua peristiwa yang mungkin memengaruhi objek dalam bucket target. Mengkonfigurasi log untuk ditempatkan di bucket terpisah memungkinkan akses ke informasi log, yang dapat berguna dalam alur kerja keamanan dan respons insiden.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM pertama-tama menggunakan logika kustom untuk mencari bucket tempat CloudTrail log Anda disimpan dan kemudian menggunakan aturan AWS Config terkelola untuk memeriksa apakah logging diaktifkan.

Jika CloudTrail mengirimkan file log dari beberapa Akun AWS ke dalam satu bucket Amazon S3 tujuan, Security Hub CSPM mengevaluasi kontrol ini hanya terhadap bucket tujuan di Wilayah tempatnya berada. Ini merampingkan temuan Anda. Namun, Anda harus mengaktifkan CloudTrail semua akun yang mengirimkan log ke bucket tujuan. Untuk semua akun kecuali akun yang menyimpan bucket tujuan, status kontrolnya adalah Tidak ada data.

Remediasi

Untuk mengaktifkan pencatatan akses server untuk bucket CloudTrail S3 Anda, lihat Mengaktifkan log akses server Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[CloudTrail.9] CloudTrail jejak harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CloudTrail::Trail`

AWS Configaturan: `tagged-cloudtrail-trail` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah AWS CloudTrail jejak memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika jejak tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika jejak tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CloudTrail jejak, lihat AddTagsdi Referensi AWS CloudTrail API.

[CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys

Persyaratan terkait: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CloudTrail::EventDataStore`

AWS Configaturan: event-data-store-cmk-encryption-enabled

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`kmsKeyArns`	Daftar Nama Sumber Daya Amazon (ARN) AWS KMS keys untuk disertakan dalam evaluasi. Kontrol menghasilkan `FAILED` temuan jika penyimpan	StringList (maksimal 3 item)	1—3 ARN kunci KMS yang ada. Sebagai contoh: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-3`	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	an data peristiwa tidak dienkripsi dengan kunci KMS dalam daftar.		`4cd-56ef-123456789 0ab` .	

Kontrol ini memeriksa apakah penyimpanan data acara AWS CloudTrail Lake dienkripsi saat istirahat dengan pelanggan yang dikelola. AWS KMS key Kontrol gagal jika penyimpanan data peristiwa tidak dienkripsi dengan kunci KMS yang dikelola pelanggan. Anda dapat secara opsional menentukan daftar kunci KMS untuk kontrol untuk disertakan dalam evaluasi.

Secara default, AWS CloudTrail Lake mengenkripsi penyimpanan data peristiwa dengan kunci terkelola Amazon S3 SSE-S3 (), menggunakan algoritme. AES-256 Untuk kontrol tambahan, Anda dapat mengonfigurasi CloudTrail Lake untuk mengenkripsi penyimpanan data peristiwa dengan customer managed AWS KMS key (SSE-KMS) sebagai gantinya. Kunci KMS yang dikelola pelanggan adalah kunci AWS KMS key yang Anda buat, miliki, dan kelola di AndaAkun AWS. Anda memiliki kontrol penuh atas jenis kunci KMS ini. Ini termasuk mendefinisikan dan memelihara kebijakan kunci, mengelola hibah, memutar materi kriptografi, menetapkan tag, membuat alias, dan mengaktifkan dan menonaktifkan kunci. Anda dapat menggunakan kunci KMS yang dikelola pelanggan dalam operasi kriptografi untuk CloudTrail data Anda dan penggunaan audit dengan CloudTrail log.

Remediasi

Untuk informasi tentang mengenkripsi penyimpanan data peristiwa AWS CloudTrail Lake dengan AWS KMS key yang Anda tentukan, lihat Memperbarui penyimpanan data peristiwa di AWS CloudTrailPanduan Pengguna. Setelah Anda mengaitkan penyimpanan data peristiwa dengan kunci KMS, kunci KMS tidak dapat dihapus atau diubah.

Kontrol CSPM Hub Keamanan untuk Amazon CloudWatch

AWS Security Hub CSPM Kontrol ini mengevaluasi CloudWatch layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/1.1, Benchmark AWS Yayasan CIS v1.2. 0/3.3, Benchmark AWS Yayasan CIS v1.4. 0/1.7, Benchmark Yay AWS asan CIS v1.4. 0/4.3, NIST.800-171.r2 3.14.6, 3. NIST.800-171.r2 14.7, PCI DSS v3.2. 1/7.2.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Pengguna root memiliki akses tidak terbatas ke semua layanan dan sumber daya dalam. Akun AWS Kami sangat menyarankan Anda menghindari menggunakan pengguna root untuk tugas sehari-hari. Meminimalkan penggunaan pengguna root dan mengadopsi prinsip hak istimewa paling sedikit untuk manajemen akses mengurangi risiko perubahan yang tidak disengaja dan pengungkapan kredenSIAL yang sangat istimewa yang tidak diinginkan.

Sebagai praktik terbaik, gunakan kredentif pengguna root Anda hanya jika diperlukan untuk melakukan tugas manajemen akun dan layanan. Terapkan kebijakan AWS Identity and Access Management (IAM) secara langsung ke grup dan peran tetapi bukan pengguna. Untuk tutorial tentang cara mengatur administrator untuk penggunaan sehari-hari, lihat Membuat pengguna dan grup admin IAM pertama Anda di Panduan Pengguna IAM

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 1.7 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.

Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:

- Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai dengan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.

2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.1, NIST.800-171.r2 3.13.1, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:
`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,
`AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk panggilan API yang tidak sah. Memantau panggilan API yang tidak sah membantu mengungkapkan kesalahan aplikasi dan dapat mengurangi waktu untuk mendeteksi aktivitas berbahaya.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 3.1 di CIS Foun AWS dations Benchmark v1.2. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.

- Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai dengan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan login konsol alarm yang tidak dilindungi oleh MFA. Pemantauan untuk login konsol faktor tunggal meningkatkan visibilitas ke akun yang tidak dilindungi oleh MFA.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 3.2 di CIS Foun AWS dations Benchmark v1.2. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya.

Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang dirujuk, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }`
Namespace metrik	**`LogMetrics`**

Bidang	Nilai
Nilai metrik	**1**
Nilai default	**0**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*your-metric-name* ...	Greater/Equal
lebih dari...	**1**

[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.4, Tolok Ukur AWS Yayasan CIS v1.4. 0/4.4, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda memantau panggilan API secara real time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS menyarankan Anda membuat filter metrik dan alarm untuk perubahan yang dilakukan pada kebijakan IAM. Pemantauan perubahan ini membantu memastikan bahwa kontrol otentikasi dan otorisasi tetap utuh.

Note

Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:

- Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang dirujuk,
atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon.
`ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

> **Note**
>
> Pola filter yang kami rekomendasikan dalam langkah-langkah remediasi ini berbeda dari pola filter dalam panduan CIS. Filter yang kami rekomendasikan hanya menargetkan peristiwa yang berasal dari panggilan API IAM.

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) || ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) || ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRolePolicy) || ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) || ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) || ($.eventN`

Bidang	Nilai
	`ame=DeletePolicyVersion) || ($.eventName=AttachRolePoli cy) \|\| ($.eventName=Detac hRolePolicy) || ($.eventN ame=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) || ($.eventName=AttachGroupPol icy) \|\| ($.eventName=Detac hGroupPolicy))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.5, Benchmark Yay AWS asan CIS v1.4. 0/4.5, NIST.800-171.r2 3.3.8, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:
`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,
`AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pengaturan CloudTrail konfigurasi. Memantau perubahan ini membantu memastikan visibilitas berkelanjutan terhadap aktivitas di akun.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.5 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) ||`

Bidang	Nilai
	`($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) || ($.eventName=StopLogging)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.6, Benchmark Yay AWS asan CIS v1.4. 0/4.6, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk upaya otentikasi konsol yang gagal. Memantau login konsol yang gagal dapat mengurangi waktu tunggu untuk mendeteksi upaya untuk memaksa kredensi secara brute-force, yang mungkin memberikan indikator, seperti IP sumber, yang dapat Anda gunakan dalam korelasi peristiwa lainnya.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.6 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota.

Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*your-metric-name* ...	Greater/Equal
lebih dari...	**1**

[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.7, Benchmark Yay AWS asan CIS v1.4. 0/4.7, NIST.800-171.r2 3.13.10, 3.13.16, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk kunci yang dikelola pelanggan yang telah mengubah status menjadi dinonaktifkan atau penghapusan terjadwal. Data yang dienkripsi dengan kunci yang dinonaktifkan atau dihapus tidak lagi dapat diakses.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.7 di CIS Foun AWS

dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik. Kontrol juga gagal jika `ExcludeManagementEventSources` berisik`kms.amazonaws.com`.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
>   Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.
>
> Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai dengan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) || ($.eventName=ScheduleKeyDeletion))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.8, Benchmark Yay AWS asan CIS v1.4. 0/4.8, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan kebijakan bucket S3. Pemantauan perubahan ini dapat mengurangi waktu untuk mendeteksi dan memperbaiki kebijakan permisif pada bucket S3 sensitif.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.8 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:

- Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai dengan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) || ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) || ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) || ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) || ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.9, Benchmark Yay AWS asan CIS v1.4. 0/4.9, NIST.800-171.r2 3.3.8, 3.14.6, NIST.800-171.r2 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pengaturan AWS Config konfigurasi. Memantau perubahan ini membantu memastikan visibilitas item konfigurasi yang berkelanjutan di akun.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.9 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:

- Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang dirujuk, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.

3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) || ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) || ($.eventName=PutConfigurationRecorder))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.10, Benchmark Yay AWS asan CIS v1.4. 0/4.10, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:
`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,
`AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai. Grup keamanan adalah filter paket stateful yang mengontrol lalu lintas masuk dan keluar dalam VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada grup keamanan. Memantau perubahan ini membantu memastikan bahwa sumber daya dan layanan tidak terekspos secara tidak sengaja.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.10 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang dirujuk, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventName=AuthorizeSecu rityGroupIngress) \|\| ($.eventN`

Bidang	Nilai
	`ame=AuthorizeSecurityGroupEgress) || ($.eventName=RevokeSecurityGroupIngress) \|\| ($.eventName=RevokeSecurityGroupEgress) || ($.eventName=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurityGroup)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.11, Benchmark Yay AWS asan CIS v1.4. 0/4.11, NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya:
`AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`,
`AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai. NACL digunakan sebagai filter paket stateless untuk mengontrol lalu lintas masuk dan keluar untuk subnet dalam VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan NACL. Memantau perubahan ini membantu memastikan bahwa AWS sumber daya dan layanan tidak terekspos secara tidak sengaja.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.11 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventName=CreateNetwork Acl) \|\| ($.eventName=Creat`

Bidang	Nilai
	`eNetworkAclEntry) || ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) || ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.12, Benchmark Yay AWS asan CIS v1.4. 0/4.12, NIST.800-171.r2 3.3.1, 3.13.1 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai. Gateway jaringan diperlukan untuk mengirim dan menerima lalu lintas ke tujuan di luar VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada gateway jaringan. Pemantauan perubahan ini membantu memastikan bahwa semua lalu lintas masuk dan keluar melintasi perbatasan VPC melalui jalur yang terkontrol.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.12 di CIS Foundations Benchmark v1.2 AWS . Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
> Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan

hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) || ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternet`

Bidang	Nilai
	`Gateway) || ($.eventName=Delet eInternetGateway) \|\| ($.eventN ame=DetachInternetGateway)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.13, Benchmark Yay AWS asan CIS v1.4. 0/4.13, NIST.800-171.r2 3.3.1, 3. NIST.800-171.r2 13.1, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda memantau panggilan API secara real time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai. Tabel routing merutekan lalu lintas jaringan antara subnet dan ke gateway jaringan.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada tabel rute. Pemantauan perubahan ini membantu memastikan bahwa semua lalu lintas VPC mengalir melalui jalur yang diharapkan.

Note

Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:

- Tidak ada jejak yang dikonfigurasi.
- Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.

Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:

- Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

  Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol `NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

> **Note**
>
> Pola filter yang kami rekomendasikan dalam langkah-langkah remediasi ini berbeda dari pola filter dalam panduan CIS. Filter yang kami rekomendasikan hanya menargetkan peristiwa yang berasal dari panggilan API Amazon Elastic Compute Cloud (EC2).

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) || ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) || ($.eventN`

Bidang	Nilai
	`ame=ReplaceRouteTableAssoci ation) || ($.eventName=Delet eRouteTable) \|\| ($.eventN ame=DeleteRoute) || ($.eventN ame=DisassociateRouteTable))}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

Persyaratan terkait: CIS Foun AWS dations Benchmark v1.2. 0/3.14, Benchmark Yay AWS asan CIS v1.4. 0/4.14, NIST.800-171.r2 3.3.1, 3. NIST.800-171.r2 13.1, 3.14.6, 3.14.7 NIST.800-171.r2 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Logs::MetricFilter`,`AWS::CloudWatch::Alarm`,`AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter: Tidak ada

Anda dapat melakukan pemantauan panggilan API secara real-time dengan mengarahkan CloudTrail CloudWatch log ke Log dan menetapkan filter dan alarm metrik yang sesuai. Anda dapat memiliki lebih dari satu VPC dalam akun, dan Anda dapat membuat koneksi peer antara dua VPC, memungkinkan lalu lintas jaringan untuk merutekan antar VPC.

CIS merekomendasikan agar Anda membuat filter metrik dan alarm untuk perubahan pada VPC. Pemantauan perubahan ini membantu memastikan bahwa kontrol otentikasi dan otorisasi tetap utuh.

Untuk menjalankan pemeriksaan ini, Security Hub CSPM menggunakan logika khusus untuk melakukan langkah-langkah audit yang tepat yang ditentukan untuk kontrol 4.14 di CIS Foun AWS dations Benchmark v1.4.0. Kontrol ini gagal jika filter metrik tepat yang ditentukan oleh CIS tidak digunakan. Bidang atau istilah tambahan tidak dapat ditambahkan ke filter metrik.

> **Note**
>
> Ketika Security Hub CSPM melakukan pemeriksaan untuk kontrol ini, ia mencari CloudTrail jejak yang digunakan akun saat ini. Jalur ini mungkin jalur organisasi milik akun lain. Multi-Region jalur juga mungkin berbasis di Wilayah yang berbeda.
> Pemeriksaan menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tidak ada jejak yang dikonfigurasi.
> - Jalur yang tersedia yang ada di Wilayah saat ini dan yang dimiliki oleh rekening giro tidak memenuhi persyaratan kontrol.
>
> Pemeriksaan menghasilkan status kontrol `NO_DATA` dalam kasus-kasus berikut:
>
> - Jalur multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak berbasis.
> - Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.
>
> Sebagai praktik terbaik, gunakan jalur organisasi untuk mencatat peristiwa dari banyak akun dalam organisasi. Jejak organisasi adalah jalur multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang di CloudTrail delegasikan. Menggunakan jejak organisasi menghasilkan status kontrol

`NO_DATA` untuk kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator yang didelegasikan CSPM Hub Keamanan Anda dengan menggunakan agregasi lintas wilayah.

Untuk alarm, akun saat ini harus memiliki topik Amazon SNS yang direferensikan, atau harus mendapatkan akses ke topik Amazon SNS dengan menelepon. `ListSubscriptionsByTopic` Jika tidak, Security Hub CSPM menghasilkan `WARNING` temuan untuk kontrol.

Remediasi

Untuk melewati kontrol ini, ikuti langkah-langkah berikut untuk membuat topik Amazon SNS, AWS CloudTrail jejak, filter metrik, dan alarm untuk filter metrik.

1. Buat topik Amazon SNS. Untuk petunjuk, lihat Mem ulai Amazon SNS di Panduan Pengembang Layanan Pem beritahuan Sederhana Amazon. Buat topik yang menerima semua alarm CIS, dan buat setidaknya satu langganan ke topik tersebut.
2. Buat CloudTrail jejak yang berlaku untuk semua Wilayah AWS. Untuk petunjuk, lihat Membuat jejak di Panduan AWS CloudTrail Pengguna.

   Catat nama grup log CloudWatch log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut di langkah berikutnya.
3. Membuat sebuah filter metrik. Untuk petunjuk, lihat Membuat filter metrik untuk grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Tentukan pola, Pola Filter	`{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) || ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) || ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventN`

Bidang	Nilai
	`ame=DeleteVpcPeeringConnection) || ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) || ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) || ($.eventName=EnableVpcClassicLink)}`
Namespace metrik	**`LogMetrics`**
Nilai metrik	**`1`**
Nilai default	**`0`**

4. Buat alarm berdasarkan filter. Untuk petunjuk, lihat Membuat CloudWatch alarm berdasarkan filter metrik grup log di Panduan CloudWatch Pengguna Amazon. Gunakan nilai berikut:

Bidang	Nilai
Kondisi, Jenis ambang	Statis
Kapan pun*`your-metric-name`* ...	Greater/Equal
lebih dari...	**`1`**

[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4 (1), NIST.800-53.r5 IR-4 (5),, NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.3.4, 3.14.6 NIST.800-171.r2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudWatch::Alarm`

AWS Config aturan: `cloudwatch-alarm-action-check`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`alarmActionRequired`	Kontrol menghasilkan tem `PASSED` uan jika parameter disetel ke `true` dan alarm memiliki tindakan ketika status alarm berubah menjadi`ALARM`.	Boolean	Tidak dapat disesuaikan	`true`
`insufficientDataActionRequired`	Kontrol menghasilkan tem `PASSED` uan jika parameter disetel ke `true` dan alarm memiliki tindakan ketika status alarm berubah menjadi`INSUFFICIENT_DATA` .	Boolean	`true` atau `false`	`false`
`okActionRequired`	Kontrol menghasilkan tem `PASSED` uan jika parameter disetel ke `true` dan alarm memiliki tindakan ketika status alarm berubah menjadi`OK`.	Boolean	`true` atau `false`	`false`

Kontrol ini memeriksa apakah CloudWatch alarm Amazon memiliki setidaknya satu tindakan yang dikonfigurasi untuk `ALARM` status. Kontrol gagal jika alarm tidak memiliki tindakan yang dikonfigurasi untuk `ALARM` status. Secara opsional, Anda dapat menyertakan nilai parameter khusus untuk juga memerlukan tindakan alarm untuk `INSUFFICIENT_DATA` status `OK` atau.

> **Note**
>
> Security Hub CSPM mengevaluasi kontrol ini berdasarkan alarm CloudWatch metrik. Alarm metrik dapat menjadi bagian dari alarm komposit yang memiliki tindakan yang ditentukan dikonfigurasi. Kontrol menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tindakan yang ditentukan tidak dikonfigurasi untuk alarm metrik.
> - Alarm metrik adalah bagian dari alarm komposit yang memiliki tindakan yang ditentukan dikonfigurasi.

Kontrol ini berfokus pada apakah CloudWatch alarm memiliki tindakan alarm yang dikonfigurasi, sedangkan CloudWatch.17 berfokus pada status aktivasi tindakan CloudWatch alarm.

Kami merekomendasikan tindakan CloudWatch alarm untuk memperingatkan Anda secara otomatis ketika metrik yang dipantau berada di luar ambang batas yang ditentukan. Alarm pemantauan membantu Anda mengidentifikasi aktivitas yang tidak biasa dan dengan cepat menanggapi masalah keamanan dan operasional ketika alarm masuk ke keadaan tertentu. Jenis tindakan alarm yang paling umum adalah memberi tahu satu atau lebih pengguna dengan mengirim pesan ke topik Amazon Simple Notification Service (Amazon SNS).

Remediasi

Untuk informasi tentang tindakan yang didukung oleh CloudWatch alarm, lihat Tind akan alarm di Panduan CloudWatch Pengguna Amazon.

[CloudWatch.16] CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu

Kategori: Identifikasi > Pencatatan

Persyaratan terkait: NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-11,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Logs::LogGroup`

AWS Config aturan: `cw-loggroup-retention-period-check`

Jenis jadwal: Ber kala

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan	
`minRetentionTime`	Periode retensi minimum dalam hari untuk CloudWatch grup log	Enum	`365, 400, 545, 731, 1827, 3653`	`365`	

Kontrol ini memeriksa apakah grup CloudWatch log Amazon memiliki periode penyimpanan setidaknya jumlah hari yang ditentukan. Kontrol gagal jika periode retensi kurang dari jumlah yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi, Security Hub CSPM menggunakan nilai default 365 hari.

CloudWatch Log memusatkan log dari semua sistem Anda, aplikasi, dan Layanan AWS dalam satu layanan yang sangat skalabel. Anda dapat menggunakan CloudWatch Log untuk memantau, menyimpan, dan mengakses file log dari instans Amazon Elastic Compute Cloud (EC2) AWS CloudTrail, Amazon Route 53, dan sumber lainnya. Mempertahankan log Anda setidaknya selama 1 tahun dapat membantu Anda mematuhi standar retensi log.

Remediasi

Untuk mengonfigurasi pengaturan penyimpanan log, lihat Meng ubah retensi data CloudWatch log di Log di Panduan CloudWatch Pengguna Amazon.

[CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan

Kategori: Deteksi > Layanan deteksi

Persyaratan terkait: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4 (12)

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CloudWatch::Alarm`

AWS Config aturan: `cloudwatch-alarm-action-enabled-check`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tindakan CloudWatch alarm diaktifkan (`ActionEnabled`harus disetel ke true). Kontrol gagal jika tindakan alarm untuk CloudWatch alarm dinonaktifkan.

> **Note**
>
> Security Hub CSPM mengevaluasi kontrol ini berdasarkan alarm CloudWatch metrik. Alarm metrik dapat menjadi bagian dari alarm komposit yang mengaktifkan tindakan alarm. Kontrol menghasilkan `FAILED` temuan dalam kasus-kasus berikut:
>
> - Tindakan yang ditentukan tidak dikonfigurasi untuk alarm metrik.
> - Alarm metrik adalah bagian dari alarm komposit yang mengaktifkan tindakan alarm.

Kontrol ini berfokus pada status aktivasi tindakan CloudWatch alarm, sedangkan CloudWatch.15 berfokus pada apakah ada `ALARM` tindakan yang dikonfigurasi dalam CloudWatch alarm.

Tindakan alarm secara otomatis mengingatkan Anda ketika metrik yang dipantau berada di luar ambang batas yang ditentukan. Jika tindakan alarm dinonaktifkan, tidak ada tindakan yang dijalankan saat alarm berubah status, dan Anda tidak akan diberi tahu tentang perubahan dalam metrik yang dipantau. Sebaiknya aktifkan tindakan CloudWatch alarm untuk membantu Anda merespons masalah keamanan dan operasional dengan cepat.

Remediasi

Untuk mengaktifkan tindakan CloudWatch alarm (konsol)

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Di panel navigasi, di bawah Alarm, pilih Semua alarm.
3. Pilih alarm yang ingin Anda aktifkan tindakannya.
4. Untuk T ind akan, pilih tindakan alarm—baru, lalu pilih Aktifkan.

Untuk informasi selengkapnya tentang mengaktifkan tindakan CloudWatch alarm, lihat Tind akan alarm di Panduan CloudWatch Pengguna Amazon.

Kontrol CSPM Security Hub untuk CodeArtifact

Kontrol CSPM Security Hub ini mengevaluasi AWS CodeArtifact layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CodeArtifact.1] CodeArtifact repositori harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeArtifact::Repository`

AWS Configaturan: `tagged-codeartifact-repository` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS CodeArtifact repositori memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika repositori tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci

tag dan gagal jika repositori tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke CodeArtifact repositori, lihat Menandai repositori CodeArtifact di Panduan Pengguna. AWS CodeArtifact

Kontrol CSPM Security Hub untuk CodeBuild

Kontrol CSPM Security Hub ini mengevaluasi AWS CodeBuild layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif

Persyaratan terkait: NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/8.2.1, PCI DSS v4.0. 1/8.3.2

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Configaturan: **`codebuild-project-source-repo-url-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah URL repositori sumber Bitbucket AWS CodeBuild proyek berisi token akses pribadi atau nama pengguna dan kata sandi. Kontrol gagal jika URL repositori sumber Bitbucket berisi token akses pribadi atau nama pengguna dan kata sandi.

> **Note**
>
> Kontrol ini mengevaluasi sumber primer dan sumber sekunder dari proyek CodeBuild pembangunan. Untuk informasi selengkapnya tentang sumber proyek, lihat Beberapa sumber input dan sampel artefak keluaran di Panduan AWS CodeBuild Pengguna.

Sign-in kredensyal tidak boleh disimpan atau ditransmisikan dalam teks yang jelas atau muncul di URL repositori sumber. Alih-alih token akses pribadi atau kredensyal masuk, Anda harus mengakses penyedia sumber Anda CodeBuild, dan mengubah URL repositori sumber Anda agar hanya berisi jalur ke lokasi repositori Bitbucket. Menggunakan token akses pribadi atau kredensyal masuk dapat mengakibatkan paparan data yang tidak diinginkan atau akses yang tidak sah.

Remediasi

Anda dapat memperbarui CodeBuild proyek Anda untuk menggunakan OAuth.

Untuk menghapus otentikasi dasar/(GitHub) Token Akses Pribadi dari sumber CodeBuild proyek

1. Buka CodeBuild konsol di https://console.aws.amazon.com/codebuild/.
2. Pilih proyek build yang berisi token akses pribadi atau nama pengguna dan kata sandi.
3. Dari Edit, pilih Sumber.
4. Pilih Putuskan sambungan GitHub dari/Bitbucket.
5. Pilih Connect menggunakan OAuth, lalu pilih Connect to GitHub/Bitbucket.
6. Saat diminta, pilih otorisasi yang sesuai.

7. Konfigurasikan ulang URL repositori Anda dan pengaturan konfigurasi tambahan, sesuai kebutuhan.
8. Pilih Perbarui sumber.

Untuk informasi selengkapnya, lihat CodeBuild menggunakan sampel berbasis kasus di AWS CodeBuildPanduan Pengguna.

[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas

Persyaratan terkait: NIST.800-53.r5 IA-5 (7), NIST.800-53.r5 SA-3, PCI DSS v3.2. 1/8.2.1, PCI DSS v4.0. 1/8.3.2

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Configaturan: **`codebuild-project-envvar-awscred-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah proyek berisi variabel lingkungan `AWS_ACCESS_KEY_ID` dan`AWS_SECRET_ACCESS_KEY`.

Kredensyal otentikasi `AWS_ACCESS_KEY_ID` dan tidak `AWS_SECRET_ACCESS_KEY` boleh disimpan dalam teks yang jelas, karena ini dapat menyebabkan paparan data yang tidak diinginkan dan akses yang tidak sah.

Remediasi

Untuk menghapus variabel lingkungan dari CodeBuild proyek, lihat Mengubah setelan proyek build AWS CodeBuild di Panduan AWS CodeBuild Pengguna. Pastikan tidak ada yang dipilih untuk variabel Lingkungan.

Anda dapat menyimpan variabel lingkungan dengan nilai sensitif di AWS Systems Manager Parameter Store atau AWS Secrets Manager kemudian mengambilnya dari spesifikasi build. Untuk petunjuk, lihat kotak berlabel Penting di bagian Lingkungan di Panduan AWS CodeBuild Pengguna.

[CodeBuild.3] CodeBuild Log S3 harus dienkripsi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/10.3.2

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Configaturan: **`codebuild-project-s3-logs-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah log Amazon S3 untuk AWS CodeBuild proyek dienkripsi. Kontrol gagal jika enkripsi dinonaktifkan untuk log S3 untuk sebuah CodeBuild proyek.

Enkripsi data saat istirahat adalah praktik terbaik yang disarankan untuk menambahkan lapisan manajemen akses di sekitar data Anda. Mengenkripsi log saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi oleh AWS akan mengakses data yang disimpan pada disk. Ini menambahkan satu set kontrol akses untuk membatasi kemampuan pengguna yang tidak sah untuk mengakses data.

Remediasi

Untuk mengubah setelan enkripsi log S3 CodeBuild proyek, lihat Mengubah setelan proyek build AWS CodeBuild di Panduan AWS CodeBuild Pengguna.

[CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Configaturan: **`codebuild-project-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah lingkungan CodeBuild proyek memiliki setidaknya satu opsi log, baik untuk S3 atau CloudWatch log diaktifkan. Kontrol ini gagal jika lingkungan CodeBuild proyek tidak memiliki setidaknya satu opsi log diaktifkan.

Dari perspektif keamanan, logging adalah fitur penting untuk memungkinkan upaya forensik masa depan dalam kasus insiden keamanan apa pun. Mengkorelasikan anomali dalam CodeBuild proyek dengan deteksi ancaman dapat meningkatkan kepercayaan pada keakuratan deteksi ancaman tersebut.

Remediasi

Untuk informasi selengkapnya tentang cara mengonfigurasi setelan log CodeBuild proyek, lihat Membuat proyek build (konsol) di Panduan CodeBuild Pengguna.

[CodeBuild.5] lingkungan CodeBuild proyek seharusnya tidak mengaktifkan mode istimewa

> **Important**
>
> Security Hub CSPM menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Log perubahan untuk kontrol CSPM Security Hub.

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Kategori: Lindungi > Manajemen Akses Aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::CodeBuild::Project`

AWS Configaturan: **`codebuild-project-environment-privileged-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah lingkungan AWS CodeBuild proyek memiliki mode istimewa yang diaktifkan atau dinonaktifkan. Kontrol gagal jika lingkungan CodeBuild proyek memiliki mode istimewa diaktifkan.

Secara default, kontainer Docker tidak mengizinkan akses ke perangkat apa pun. Mode istimewa memberikan akses container Docker proyek build ke semua perangkat. Pengaturan `privilegedMode` dengan nilai `true` memungkinkan daemon Docker berjalan di dalam wadah Docker. Daemon Docker mendengarkan permintaan API Docker dan mengelola objek Docker seperti gambar, wadah, jaringan, dan volume. Parameter ini hanya boleh disetel ke true jika proyek build digunakan untuk membangun image Docker. Jika tidak, pengaturan ini harus dinonaktifkan untuk mencegah akses yang tidak diinginkan ke API Docker serta perangkat keras yang mendasarinya. Pengaturan `privilegedMode` untuk `false` membantu melindungi sumber daya penting dari gangguan dan penghapusan.

Remediasi

Untuk mengonfigurasi pengaturan lingkungan CodeBuild proyek, lihat Membuat proyek build (konsol) di Panduan CodeBuild Pengguna. Di bagian Lingkungan, jangan pilih pengaturan Privileged.

[CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::CodeBuild::ReportGroup`

AWS Configaturan: **`codebuild-report-group-encrypted-at-rest`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah hasil pengujian grup AWS CodeBuild laporan yang diekspor ke bucket Amazon Simple Storage Service (Amazon S3) dienkripsi saat istirahat. Kontrol gagal jika ekspor grup laporan tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda

melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengenkripsi ekspor grup laporan ke S3, lihat Memperbarui grup laporan di AWS CodeBuildPanduan Pengguna.

Kontrol CSPM Security Hub untuk Amazon Profiler CodeGuru

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon CodeGuru Profiler.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeGuruProfiler::ProfilingGroup`

AWS Configaturan: `codeguruprofiler-profiling-group-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah grup CodeGuru profil Amazon Profiler memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika grup

profil tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup profil tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke grup CodeGuru profil Profiler, lihat Menandai grup profil di Panduan Pengguna Amazon CodeGuru Profiler.

Kontrol CSPM Security Hub untuk Amazon Reviewer CodeGuru

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon CodeGuru Reviewer.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CodeGuruReviewer::RepositoryAssociation`

AWS Configaturan: `codegurureviewer-repository-association-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah asosiasi CodeGuru repositori Amazon Reviewer memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika asosiasi repositori tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredKeyTags` Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika asosiasi repositori tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM

(pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke asosiasi CodeGuru repositori Reviewer, lihat Menandai asosiasi repositori di Panduan Pengguna Amazon Reviewer. CodeGuru

Kontrol CSPM Hub Keamanan untuk Amazon Cognito

AWS Security Hub CSPM Kontrol ini mengevaluasi layanan dan sumber daya Amazon Cognito. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar

Kategori: Lindungi > Manajemen akses aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Cognito::UserPool`

AWS Config aturan: cognito-user-pool-advanced-security-enabled

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`SecurityMode`	Mode penegakan perlindungan ancaman yang diperiksa kontrol.	String	`AUDIT`, `ENFORCED`	`ENFORCED`

Kontrol ini memeriksa apakah kumpulan pengguna Amazon Cognito memiliki perlindungan ancaman yang diaktifkan dengan mode penegakan diatur ke fungsi penuh untuk otentikasi standar. Kontrol gagal jika kumpulan pengguna memiliki perlindungan ancaman yang dinonaktifkan atau jika mode penegakan tidak disetel ke fungsi penuh untuk otentikasi standar. Kecuali Anda memberikan nilai parameter kustom, Security Hub CSPM menggunakan nilai default `ENFORCED` untuk mode penegakan yang disetel ke fungsi penuh untuk otentikasi standar.

Setelah membuat kumpulan pengguna Amazon Cognito, Anda dapat mengaktifkan perlindungan ancaman dan menyesuaikan tindakan yang diambil sebagai respons terhadap risiko yang berbeda. Atau, Anda dapat menggunakan mode audit untuk mengumpulkan metrik pada risiko yang terdeteksi tanpa menerapkan mitigasi keamanan apa pun. Dalam mode audit, perlindungan ancaman menerbitkan metrik ke Amazon CloudWatch. Anda dapat melihat metrik setelah Amazon Cognito menghasilkan acara pertamanya.

Remediasi

Untuk informasi tentang mengaktifkan perlindungan ancaman untuk kumpulan pengguna Amazon Cognito, lihat Keamanan lanjutan dengan perlindungan ancaman di Panduan Pengembang Amazon Cognito.

[Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi

Kategori: L indungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Cognito::IdentityPool`

AWS Config aturan: cognito-identity-pool-unauth-access-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kumpulan identitas Amazon Cognito dikonfigurasi untuk mengizinkan identitas yang tidak diautentikasi. Kontrol gagal jika akses tamu diaktifkan (`AllowUnauthenticatedIdentities`parameter disetel ke`true`) untuk kumpulan identitas.

Jika kumpulan identitas Amazon Cognito mengizinkan identitas yang tidak diautentikasi, kumpulan identitas menyediakan AWS kredentif sementara kepada pengguna yang belum diautentikasi melalui penyedia identitas (tamu). Ini menciptakan risiko keamanan karena memungkinkan akses anonim ke AWS sumber daya. Jika Anda menonaktifkan akses tamu, Anda dapat membantu memastikan bahwa hanya pengguna yang diautentikasi dengan benar yang dapat mengakses AWS sumber daya Anda, sehingga mengurangi risiko akses tidak sah dan potensi pelanggaran keamanan. Sebagai praktik terbaik, kumpulan identitas harus memerlukan otentikasi melalui penyedia identitas yang didukung. Jika akses yang tidak diautentikasi diperlukan, penting untuk secara hati-hati membatasi izin untuk identitas yang tidak diautentikasi, dan secara teratur meninjau dan memantau penggunaannya.

Remediasi

Untuk informasi tentang menonaktifkan akses tamu untuk kumpulan identitas Amazon Cognito, lihat Mengaktifkan atau menonaktifkan akses tamu di Panduan Pengembang Amazon Cognito.

[Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat

Kategori: Lindungi > Manajemen akses aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Cognito::UserPool`

AWS Config aturan: cognito-user-pool-password-policy-check

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`minLength`	Jumlah minimum karakter yang harus berisi kata sandi.	Bilangan Bulat	8 untuk 99	8
`requireLowercase`	Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi.	Boolean	`True`, `False`	`True`
`requireUppercase`	Memerlukan setidaknya satu karakter huruf besar dalam kata sandi.	Boolean	`True`, `False`	`True`
`requireNumbers`	Memerlukan setidaknya satu nomor dalam kata sandi.	Boolean	`True`, `False`	`True`
`requireSymbols`	Memerlukan setidaknya satu simbol dalam kata sandi.	Boolean	`True`, `False`	`True`
`temporaryPasswordValidity`	Jumlah hari maksimum kata sandi dapat ada sebelum kedaluwarsa.	Bilangan Bulat	1 untuk 365	7

Kontrol ini memeriksa apakah kebijakan kata sandi untuk kumpulan pengguna Amazon Cognito memerlukan penggunaan kata sandi yang kuat, berdasarkan pengaturan yang disarankan untuk kebijakan kata sandi. Kontrol gagal jika kebijakan kata sandi untuk kumpulan pengguna tidak memerlukan kata sandi yang kuat. Secara opsional, Anda dapat menentukan nilai kustom untuk pengaturan kebijakan yang diperiksa kontrol.

Kata sandi yang kuat adalah praktik terbaik keamanan untuk kumpulan pengguna Amazon Cognito. Kata sandi yang lemah dapat mengekspos kredenSIAL pengguna ke sistem yang menebak kata sandi dan mencoba mengakses data. Hal ini terutama berlaku untuk aplikasi yang terbuka untuk internet. Kebijakan kata sandi adalah elemen sentral dari keamanan direktori pengguna. Dengan menggunakan kebijakan kata sandi, Anda dapat mengonfigurasi kumpulan pengguna

agar memerlukan kompleksitas kata sandi dan pengaturan lain yang sesuai dengan standar dan persyaratan keamanan Anda.

Remediasi

Untuk informasi tentang membuat atau memperbarui kebijakan kata sandi untuk kumpulan pengguna Amazon Cognito, lihat Men ambahkan persyaratan kata sandi kumpulan pengguna di Panduan Pengembang Amazon Cognito.

[Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus

Kategori: Lindungi > Manajemen akses aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Cognito::UserPool`

AWS Config aturan: cognito-userpool-cust-auth-threat-full-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kumpulan pengguna Amazon Cognito memiliki perlindungan ancaman yang diaktifkan dengan mode penegakan diatur ke fungsi penuh untuk otentikasi kustom. Kontrol gagal jika kumpulan pengguna memiliki perlindungan ancaman yang dinonaktifkan atau jika mode penegakan tidak disetel ke fungsi penuh untuk otentikasi kustom.

Perlindungan ancaman, sebelumnya disebut fitur keamanan lanjutan, adalah seperangkat alat pemantauan untuk aktivitas yang tidak diinginkan di kumpulan pengguna Anda, dan alat konfigurasi untuk secara otomatis mematikan aktivitas yang berpotensi berbahaya. Setelah membuat kumpulan pengguna Amazon Cognito, Anda dapat mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus dan menyesuaikan tindakan yang diambil sebagai respons terhadap risiko yang berbeda. Full-function mode mencakup serangkaian reaksi otomatis untuk mendeteksi aktivitas yang tidak diinginkan dan kata sandi yang dikompromikan.

Remediasi

Untuk informasi tentang mengaktifkan perlindungan ancaman untuk kumpulan pengguna Amazon Cognito, lihat Keamanan lanjutan dengan perlindungan ancaman di Panduan Pengembang Amazon Cognito.

[Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito

Kategori: L indungi > Manajemen akses aman > Multi-factor otentikasi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Cognito::UserPool`

AWS Config aturan: cognito-user-pool-mfa-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kumpulan pengguna Amazon Cognito yang dikonfigurasi dengan kebijakan masuk hanya kata sandi mengaktifkan otentikasi multi-faktor (MFA). Kontrol gagal jika kumpulan pengguna yang dikonfigurasi dengan kebijakan masuk hanya kata sandi tidak mengaktifkan MFA.

Multi-factor otentikasi (MFA) menambahkan sesuatu yang Anda miliki faktor otentikasi ke faktor sesuatu yang Anda ketahui (biasanya nama pengguna dan kata sandi). Untuk pengguna federasi, Amazon Cognito mendelegasikan otentikasi ke penyedia identitas (IdP) dan tidak menawarkan faktor otentikasi tambahan. Namun, jika Anda memiliki pengguna lokal dengan otentikasi kata sandi, mengonfigurasi MFA untuk kumpulan pengguna meningkatkan keamanannya.

> **Note**
>
> Kontrol ini tidak berlaku untuk pengguna federasi dan pengguna yang masuk dengan faktor tanpa kata sandi.

Remediasi

Untuk informasi tentang cara mengonfigurasi MFA untuk kumpulan pengguna Amazon Cognito, lihat Men ambahkan MFA ke kumpulan pengguna di Panduan Pengembang Amazon Cognito.

[Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan

Kategori: Mel indungi > Perlindungan Data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Cognito::UserPool`

AWS Config aturan: cognito-user-pool-deletion-protection-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kumpulan pengguna Amazon Cognito mengaktifkan perlindungan penghapusan. Kontrol gagal jika perlindungan penghapusan dinonaktifkan untuk kumpulan pengguna.

Perlindungan penghapusan membantu memastikan bahwa kumpulan pengguna Anda tidak dihapus secara tidak sengaja. Saat Anda mengonfigurasi kumpulan pengguna dengan perlindungan penghapusan, kumpulan tidak dapat dihapus oleh pengguna mana pun. Perlindungan penghapusan mencegah Anda meminta penghapusan kumpulan pengguna kecuali jika Anda terlebih dahulu mengubah kumpulan dan menonaktifkan perlindungan penghapusan.

Remediasi

Untuk mengonfigurasi perlindungan penghapusan untuk kumpulan pengguna Amazon Cognito, lihat Perlindungan penghapusan kumpulan pengguna di Panduan Pengembang Amazon Cognito.

Kontrol CSPM Hub Keamanan untuk AWS Config

Kontrol CSPM Hub Keamanan ini mengevaluasi AWS Config layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya

> **Note**
>
> Ketika Security Hub CSPM dan Security Hub diaktifkan, Config.1 aturan akan selalu memiliki status PASSED. Ini karena Security Hub CSPM memiliki akses langsung ke item konfigurasi melalui perekam konfigurasi terkait layanan. Parameter untuk kontrol ini tidak berlaku karena perekam konfigurasi terkait layanan internal secara otomatis dibuat dengan peran terkait layanan AWS Config . Untuk informasi selengkapnya, lihat Menggunakan perekam konfigurasi terkait layanan.

Kontrol multicloud (seperti kontrol Azure) dan rekaman sumber daya terkaitnya tidak diperhitungkan dalam evaluasi. Config.1 Standar multicloud selalu menggunakan perekam konfigurasi tertaut layanan internal yang disiapkan konektor multicloud CSPM secara otomatis, terlepas dari status pengaktifan Hub Keamanan. Karena perekaman multicloud sepenuhnya dikelola oleh konektor, itu tidak mempengaruhi status Config.1 kepatuhan. Config.1 hanya mengevaluasi konfigurasi perekaman AWS sumber daya.

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/3.3, Benchmark AWS Yayasan CIS v1.2. 0/2.5, Benchmark Yay AWS asan CIS v1.4. 0/3.5, Benchmark Yay AWS asan CIS v3.0. 0/3.3, NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (2), PCI DSS v3.2. 1/10.5.2, PCI DSS v3.2. 1/11.5

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: Tidak ada (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Ber kala

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`includeConfigServiceLinkedRoleCheck`	Kontrol tidak mengevaluasi apakah AWS Config menggunakan peran terkait layanan jika parameter disetel ke. `false`	Boolean	`true` atau `false`	`true`

Kontrol ini memeriksa apakah AWS Config diaktifkan di akun Anda saat ini Wilayah AWS, mencatat semua sumber daya yang sesuai dengan kontrol yang diaktifkan di Wilayah saat ini, dan menggunakan peran terkait layanan AWS Config . Nama peran terkait layanan adalah.

AWSServiceRoleForConfig Jika Anda tidak menggunakan peran yang ditautkan layanan dan tidak menyetel `includeConfigServiceLinkedRoleCheck` parameter `kefalse`, kontrol gagal karena peran lain mungkin tidak memiliki izin yang diperlukan AWS Config untuk merekam sumber daya Anda secara akurat.

AWS Config Layanan ini melakukan manajemen konfigurasi AWS sumber daya yang didukung di akun Anda dan mengirimkan file log kepada Anda. Informasi yang direkam mencakup item konfigurasi (AWS sumber daya), hubungan antara item konfigurasi, dan setiap perubahan konfigurasi dalam sumber daya. Sumber daya global adalah sumber daya yang tersedia di Wilayah mana pun.

Kontrol dievaluasi sebagai berikut:

- Jika Wilayah saat ini ditetapkan sebagai Wilayah agregasi Anda, kontrol menghasilkan `PASSED` temuan hanya jika sumber daya global AWS Identity and Access Management (IAM) dicatat (jika Anda telah mengaktifkan kontrol yang memerlukannya).
- Jika Wilayah saat ini disetel sebagai Wilayah tertaut, kontrol tidak mengevaluasi apakah sumber daya global IAM dicatat.
- Jika Wilayah saat ini tidak ada di agregator Anda, atau jika agregasi lintas wilayah tidak diatur di akun Anda, kontrol menghasilkan `PASSED` temuan hanya jika sumber daya global IAM dicatat (jika Anda telah mengaktifkan kontrol yang memerlukannya).

Hasil kontrol tidak terpengaruh oleh apakah Anda memilih pencatatan harian atau terus menerus dari perubahan status sumber daya di AWS Config. Namun, hasil kontrol ini dapat berubah saat kontrol baru dirilis jika Anda telah mengonfigurasi pengaktifan otomatis kontrol baru atau memiliki kebijakan konfigurasi pusat yang secara otomatis mengaktifkan kontrol baru. Dalam kasus ini, jika Anda tidak merekam semua sumber daya, Anda harus mengonfigurasi perekaman untuk sumber daya yang terkait dengan kontrol baru untuk menerima tem `PASSED` uan.

Pemeriksaan keamanan CSPM Hub Keamanan berfungsi sebagaimana dimaksud hanya jika Anda mengaktifkan AWS Config di semua Wilayah dan mengonfigurasi perekaman sumber daya untuk kontrol yang memerlukannya.

> **Note**
>
> Config.1 mengharuskan itu AWS Config diaktifkan di semua Wilayah tempat Anda menggunakan Security Hub CSPM.
> Karena Security Hub CSPM adalah layanan Regional, pemeriksaan yang dilakukan untuk kontrol ini hanya mengevaluasi Wilayah saat ini untuk akun.

Untuk mengizinkan pemeriksaan keamanan terhadap sumber daya global IAM di suatu Wilayah, Anda harus merekam sumber daya global IAM di Wilayah tersebut. Wilayah yang tidak memiliki sumber daya global IAM yang direkam akan menerima tem `PASSED` uan default untuk kontrol yang memeriksa sumber daya global IAM. Karena sumber daya global IAM identik di seluruh wilayah Wilayah AWS, sebaiknya Anda merekam sumber daya global IAM hanya di Wilayah asal (jika agregasi lintas wilayah diaktifkan di akun Anda). Sumber daya IAM hanya akan direkam di Wilayah di mana perekaman sumber daya global diaktifkan. Jenis sumber daya IAM yang direkam secara global yang AWS Config didukung adalah pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan. Anda dapat mempertimbangkan untuk menonaktifkan kontrol CSPM Security Hub yang memeriksa jenis sumber daya ini di Wilayah tempat perekaman sumber daya global dimatikan. Untuk informasi selengkapnya, lihat Kontrol yang disarankan untuk dinonaktifkan di CSPM Security Hub.

Remediasi

Di Wilayah dan Wilayah beranda yang bukan bagian dari agregator, catat semua sumber daya yang diperlukan untuk kontrol yang diaktifkan di Wilayah saat ini, termasuk sumber daya global IAM jika Anda telah mengaktifkan kontrol yang memerlukan sumber daya global IAM.

Di Wilayah tertaut, Anda dapat menggunakan mode AWS Config perekaman apa pun, selama Anda merekam semua sumber daya yang sesuai dengan kontrol yang diaktifkan di Wilayah saat ini. Di Wilayah tertaut, jika Anda telah mengaktifkan kontrol yang memerlukan perekaman sumber daya global IAM, Anda tidak akan menerima tem `FAILED` uan (rekaman sumber daya lain sudah cukup).

Bid `StatusReasons` ang dalam `Compliance` objek temuan Anda dapat membantu Anda menentukan mengapa Anda memiliki penemuan yang gagal untuk kontrol ini. Untuk informasi selengkapnya, lihat Detail kepatuhan untuk temuan kontrol.

Untuk daftar sumber daya mana yang harus dicatat untuk setiap kontrol, lihatDiperlukanAWS Configsumber daya untuk temuan kontrol. Untuk informasi umum tentang mengaktifkan AWS Config dan mengonfigurasi perekaman sumber daya, lihatMengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM.

Kontrol CSPM Security Hub untuk Amazon Connect

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon Connect.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::CustomerProfiles::ObjectType`

AWS Configaturan: `customerprofiles-object-type-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah jenis objek Amazon Connect Customer Profiles memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika jenis objek tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika jenis objek tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik

sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke jenis objek Profil Pelanggan, lihat Menambahkan tag ke sumber daya di Amazon Connect Customer di Panduan Connect Customer Administrator.

[Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Connect::Instance`

AWS Configaturan: connect-instance-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Connect Customer dikonfigurasi untuk membuat dan menyimpan log aliran dalam grup CloudWatch log Amazon. Kontrol gagal jika instance Connect Customer tidak dikonfigurasi untuk membuat dan menyimpan log alur dalam grup CloudWatch log.

Log alur Pelanggan Amazon Connect memberikan detail real-time tentang peristiwa di alur Pelanggan Amazon Connect. Alur mendefinisikan pengalaman pelanggan dengan pusat kontak Pelanggan Amazon Connect dari awal hingga akhir. Secara default, saat Anda membuat instans Pelanggan Amazon Connect baru, grup CloudWatch log Amazon dibuat secara otomatis untuk menyimpan log alur untuk instance tersebut. Log aliran dapat membantu Anda menganalisis alur, menemukan kesalahan, dan memantau metrik operasional. Anda juga dapat mengatur peringatan untuk peristiwa tertentu yang dapat terjadi dalam alur.

Remediasi

Untuk informasi tentang mengaktifkan log alur untuk instans Pelanggan Amazon Connect, lihat Mengaktifkan log alur Pelanggan Amazon Connect di grup CloudWatch log Amazon di Panduan Connect Customer Administrator.

Kontrol CSPM Security Hub untuk Amazon Data Firehose

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon Data Firehose.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::KinesisFirehose::DeliveryStream`

AWS Configaturan: **`kinesis-firehose-delivery-stream-encrypted`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah aliran pengiriman Amazon Data Firehose dienkripsi saat istirahat dengan enkripsi sisi server. Kontrol ini gagal jika aliran pengiriman Firehose tidak dienkripsi saat istirahat dengan enkripsi sisi server.

Server-side enkripsi adalah fitur dalam aliran pengiriman Amazon Data Firehose yang secara otomatis mengenkripsi data sebelum diam dengan menggunakan kunci yang dibuat di (). AWS Key Management Service AWS KMS Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Firehose Data, dan didekripsi setelah diambil dari penyimpanan. Ini memungkinkan Anda untuk mematuhi persyaratan peraturan dan meningkatkan keamanan data Anda.

Remediasi

Untuk mengaktifkan enkripsi sisi server pada aliran pengiriman Firehose, lihat Perlindungan Data di Amazon Data Firehose di Panduan Pengembang Amazon Data Firehose.

Kontrol CSPM Security Hub untukAWS Database Migration Service

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Database Migration Service (AWS DMS) dan AWS DMS sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Configaturan: dms-replication-not-public

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance AWS DMS replikasi bersifat publik. Untuk melakukan ini, ia memeriksa nilai `PubliclyAccessible` bidang.

Instance replikasi pribadi memiliki alamat IP pribadi yang tidak dapat Anda akses di luar jaringan replikasi. Sebuah contoh replikasi harus memiliki alamat IP pribadi ketika database sumber dan target berada dalam jaringan yang sama. Jaringan juga harus terhubung ke VPC instance replikasi menggunakan VPNDirect Connect,, atau VPC peering. Untuk mempelajari lebih lanjut tentang instans replikasi publik dan pribadi, lihat Instans replikasi publik dan pribadi di Panduan Pengguna. AWS Database Migration Service

Anda juga harus memastikan bahwa akses ke konfigurasi AWS DMS instans terbatas hanya untuk pengguna yang berwenang. Untuk melakukan ini, batasi izin IAM pengguna untuk mengubah AWS DMS pengaturan dan sumber daya.

Remediasi

Anda tidak dapat mengubah pengaturan akses publik untuk instance replikasi DMS setelah membuatnya. Untuk mengubah setelan akses publik, hapus instans Anda saat ini, lalu buat ulang. Jangan pilih opsi yang dapat diakses publik.

[DMS.2] Sertifikat DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::Certificate`

AWS Configaturan: `tagged-dms-certificate` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratanAWS.	

Kontrol ini memeriksa apakah AWS DMS sertifikat memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke sertifikat DMS, lihat Menandai sumber daya AWS Database Migration Service di AWS Database Migration Service Panduan Pengguna.

[DMS.3] Langganan acara DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::EventSubscription`

AWS Configaturan: `tagged-dms-eventsubscription` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah langganan AWS DMS acara memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika langganan acara tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika langganan acara tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke langganan acara DMS, lihat Menandai sumber daya AWS Database Migration Service di AWS Database Migration Service Panduan Pengguna.

[DMS.4] Contoh replikasi DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Configaturan: `tagged-dms-replicationinstance` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratanAWS.	

Kontrol ini memeriksa apakah instance AWS DMS replikasi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika instance replikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance replikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instance replikasi DMS, lihat Menandai sumber daya AWS Database Migration Service di Panduan Pengguna. AWS Database Migration Service

[DMS.5] Grup subnet replikasi DMS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DMS::ReplicationSubnetGroup`

AWS Configaturan: `tagged-dms-replicationsubnetgroup` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah grup subnet AWS DMS replikasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet replikasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet replikasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet replikasi DMS, lihat Menandai sumber daya AWS Database Migration Service di Panduan Pengguna. AWS Database Migration Service

[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Configaturan: dms-auto-minor-version-upgrade-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah upgrade versi minor otomatis diaktifkan untuk instance AWS DMS replikasi. Kontrol gagal jika upgrade versi minor otomatis tidak diaktifkan untuk instance replikasi DMS.

DMS menyediakan upgrade versi minor otomatis ke setiap mesin replikasi yang didukung sehingga Anda dapat memperbarui instance replikasi Anda. Versi minor dapat memperkenalkan fitur perangkat

lunak baru, perbaikan bug, patch keamanan, dan peningkatan kinerja. Dengan mengaktifkan pemutakhiran versi minor otomatis pada instance replikasi DMS, peningkatan kecil diterapkan secara otomatis selama jendela pemeliharaan atau segera jika opsi Terapkan segera berubah dipilih.

Remediasi

Untuk mengaktifkan pemutakhiran versi minor otomatis pada instance replikasi DMS, lihat Memodifikasi instance replikasi di Panduan Pengguna. AWS Database Migration Service

[DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationTask`

AWS Configaturan: dms-replication-task-targetdb-logging

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan dengan tingkat keparahan minimum `LOGGER_SEVERITY_DEFAULT` untuk tugas `TARGET_APPLY` replikasi DMS dan. `TARGET_LOAD` Kontrol gagal jika logging tidak diaktifkan untuk tugas-tugas ini atau jika tingkat keparahan minimum kurang dari`LOGGER_SEVERITY_DEFAULT`.

DMS menggunakan Amazon CloudWatch untuk mencatat informasi selama proses migrasi. Menggunakan pengaturan tugas logging, Anda dapat menentukan aktivitas komponen mana yang dicatat dan berapa banyak informasi yang dicatat. Anda harus menentukan pencatatan untuk tugas-tugas berikut:

- `TARGET_APPLY`— Pernyataan bahasa definisi data dan data (DDL) diterapkan ke database target.
- `TARGET_LOAD`— Data dimuat ke database target.

Logging memainkan peran penting dalam tugas replikasi DMS dengan memungkinkan pemantauan, pemecahan masalah, audit, analisis kinerja, deteksi kesalahan, dan pemulihan, serta analisis historis dan pelaporan. Ini membantu memastikan keberhasilan replikasi data antar database sambil menjaga integritas data dan kepatuhan terhadap persyaratan peraturan. Level logging selain `DEFAULT` jarang diperlukan untuk komponen ini selama pemecahan masalah. Kami merekomendasikan untuk menjaga tingkat logging seperti `DEFAULT` untuk komponen ini kecuali secara khusus diminta untuk mengubahnyaDukungan. Tingkat logging minimal `DEFAULT` memastikan bahwa pesan informasi, peringatan, dan pesan kesalahan ditulis ke log. Kontrol ini memeriksa apakah tingkat logging setidaknya salah satu dari yang berikut untuk tugas replikasi sebelumnya:`LOGGER_SEVERITY_DEFAULT`,, `LOGGER_SEVERITY_DEBUG` atau. `LOGGER_SEVERITY_DETAILED_DEBUG`

Remediasi

Untuk mengaktifkan pencatatan tugas replikasi DMS basis data target, lihat Melihat dan mengelola log AWS DMS tugas di AWS Database Migration ServicePanduan Pengguna.

[DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationTask`

AWS Configaturan: dms-replication-task-sourcedb-logging

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan dengan tingkat keparahan minimum `LOGGER_SEVERITY_DEFAULT` untuk tugas `SOURCE_CAPTURE` replikasi DMS dan. `SOURCE_UNLOAD` Kontrol gagal jika logging tidak diaktifkan untuk tugas-tugas ini atau jika tingkat keparahan minimum kurang dari`LOGGER_SEVERITY_DEFAULT`.

DMS menggunakan Amazon CloudWatch untuk mencatat informasi selama proses migrasi. Menggunakan pengaturan tugas logging, Anda dapat menentukan aktivitas komponen mana yang dicatat dan berapa banyak informasi yang dicatat. Anda harus menentukan pencatatan untuk tugas-tugas berikut:

- `SOURCE_CAPTURE`Data replikasi atau perubahan data capture (CDC) yang sedang berlangsung diambil dari database sumber atau layanan, dan diteruskan ke komponen `SORTER` layanan.
- `SOURCE_UNLOAD`— Data diturunkan dari database sumber atau layanan selama pemuatan penuh.

Logging memainkan peran penting dalam tugas replikasi DMS dengan memungkinkan pemantauan, pemecahan masalah, audit, analisis kinerja, deteksi kesalahan, dan pemulihan, serta analisis historis dan pelaporan. Ini membantu memastikan keberhasilan replikasi data antar database sambil menjaga integritas data dan kepatuhan terhadap persyaratan peraturan. Level logging selain `DEFAULT` jarang diperlukan untuk komponen ini selama pemecahan masalah. Kami merekomendasikan untuk menjaga tingkat logging seperti `DEFAULT` untuk komponen ini kecuali secara khusus diminta untuk mengubahnyaDukungan. Tingkat logging minimal `DEFAULT` memastikan bahwa pesan informasi, peringatan, dan pesan kesalahan ditulis ke log. Kontrol ini memeriksa apakah tingkat logging setidaknya salah satu dari yang berikut untuk tugas replikasi sebelumnya:`LOGGER_SEVERITY_DEFAULT`,, `LOGGER_SEVERITY_DEBUG` atau. `LOGGER_SEVERITY_DETAILED_DEBUG`

Remediasi

Untuk mengaktifkan pencatatan tugas replikasi DMS basis data sumber, lihat Melihat dan mengelola log AWS DMS tugas di AWS Database Migration ServicePanduan Pengguna.

[DMS.9] Titik akhir DMS harus menggunakan SSL

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Configaturan: dms-endpoint-ssl-configured

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir menggunakan koneksi SSL. Kontrol gagal jika titik akhir tidak menggunakan SSL.

SSL/TLS koneksi menyediakan lapisan keamanan dengan mengenkripsi koneksi antara instance replikasi DMS dan database Anda. Menggunakan sertifikat memberikan lapisan keamanan tambahan dengan memvalidasi bahwa koneksi sedang dibuat ke database yang diharapkan. Hal ini dilakukan dengan memeriksa sertifikat server yang secara otomatis diinstal pada semua instance database yang Anda berikan. Dengan mengaktifkan koneksi SSL pada titik akhir DMS Anda, Anda melindungi kerahasiaan data selama migrasi.

Remediasi

Untuk menambahkan koneksi SSL ke titik akhir DMS baru atau yang sudah ada, lihat Menggunakan SSL dengan AWS Database Migration Service di Panduan Pengguna. AWS Database Migration Service

[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6,, NIST.800-53.r5 AC-17 NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5, PCI DSS v4.0. 1/7.3.1

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Configaturan: dms-neptune-iam-authorization-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk database Amazon Neptunus dikonfigurasi dengan otorisasi IAM. Kontrol gagal jika titik akhir DMS tidak mengaktifkan otorisasi IAM.

AWS Identity and Access Management(IAM) menyediakan kontrol akses berbutir halus di seluruh. AWS Dengan IAM, Anda dapat menentukan siapa yang dapat mengakses layanan dan sumber

daya mana, dan dalam kondisi apa. Dengan kebijakan IAM, Anda mengelola izin untuk tenaga kerja dan sistem Anda untuk memastikan izin hak istimewa paling sedikit. Dengan mengaktifkan otorisasi IAM pada AWS DMS titik akhir untuk database Neptunus, Anda dapat memberikan hak otorisasi kepada pengguna IAM dengan menggunakan peran layanan yang ditentukan oleh parameter. `ServiceAccessRoleARN`

Remediasi

Untuk mengaktifkan otorisasi IAM pada titik akhir DMS untuk database Neptunus, lihat Menggunakan Amazon Neptunus sebagai target dalam Panduan Pengguna. AWS Database Migration Service AWS Database Migration Service

[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi

Persyaratan terkait: NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-6, NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-5, PCI DSS v4.0. 1/7.3.1

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Configaturan: dms-mongo-db-authentication-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk MongoDB dikonfigurasi dengan mekanisme otentikasi. Kontrol gagal jika jenis otentikasi tidak disetel untuk titik akhir.

AWS Database Migration Servicemendukung dua metode otentikasi untuk MongoDB MONGODB-CR- untuk MongoDB versi 2.x, dan untuk MongoDB versi 3.x SCRAM-SHA-1atau yang lebih baru. Metode otentikasi ini digunakan untuk mengautentikasi dan mengenkripsi kata sandi MongoDB jika pengguna ingin menggunakan kata sandi untuk mengakses database. Otentikasi pada AWS DMS titik akhir memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses dan memodifikasi data yang sedang dimigrasi antar database. Tanpa autentikasi yang tepat, pengguna yang tidak sah dapat memperoleh akses ke data sensitif selama proses migrasi. Hal ini dapat mengakibatkan pelanggaran data, kehilangan data, atau insiden keamanan lainnya.

Remediasi

Untuk mengaktifkan mekanisme otentikasi pada titik akhir DMS untuk MongoDB, lihat Menggunakan MongoDB sebagai sumber di Panduan Pengguna. AWS DMS AWS Database Migration Service

[DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS

Persyaratan terkait: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13, PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::Endpoint`

AWS Configaturan: dms-redis-tls-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DMS titik akhir untuk Redis OSS dikonfigurasi dengan koneksi TLS. Kontrol gagal jika titik akhir tidak mengaktifkan TLS.

TLS menyediakan keamanan end-to-end ketika data dikirim antara aplikasi atau database melalui internet. Saat Anda mengonfigurasi enkripsi SSL untuk titik akhir DMS Anda, ini memungkinkan komunikasi terenkripsi antara basis data sumber dan target selama proses migrasi. Ini membantu mencegah penyadapan dan intersepsi data sensitif oleh aktor jahat. Tanpa enkripsi SSL, data sensitif dapat diakses, mengakibatkan pelanggaran data, kehilangan data, atau insiden keamanan lainnya.

Remediasi

Untuk mengaktifkan koneksi TLS pada titik akhir DMS untuk Redis, lihat Menggunakan Redis sebagai target dalam Panduan Pengguna. AWS Database Migration Service AWS Database Migration Service

[DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DMS::ReplicationInstance`

AWS Configaturan: dms-replication-instance-multi-az-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance replikasi AWS Database Migration Service (AWS DMS) dikonfigurasi untuk menggunakan beberapa Availability Zones (Multi-AZ deployment). Kontrol gagal jika instance AWS DMS replikasi tidak dikonfigurasi untuk menggunakan Multi-AZ penerapan.

Dalam Multi-AZ penerapan, AWS DMS secara otomatis menyediakan dan memelihara replika siaga dari instance replikasi di Availability Zone (AZ) yang berbeda. Contoh replikasi utama kemudian direplikasi secara sinkron ke replika siaga. Jika instans replikasi utama gagal atau menjadi tidak responsif, cadangan tersebut melanjutkan tugas yang sedang berlangsung dengan gangguan minimal. Untuk informasi selengkapnya, lihat Bekerja dengan instance replikasi di Panduan AWS Database Migration Service Pengguna.

Remediasi

Setelah Anda membuat instance AWS DMS replikasi, Anda dapat mengubah setelan Multi-AZ penerapan untuk itu. Untuk informasi tentang mengubah ini dan setelan lainnya untuk instance replikasi yang ada, lihat Memodifikasi instance replikasi di Panduan Pengguna. AWS Database Migration Service

Kontrol CSPM Security Hub untukAWS DataSync

Kontrol CSPM Security Hub ini mengevaluasi AWS DataSync layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DataSync.1] DataSync tugas harus mengaktifkan logging

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DataSync::Task`

AWS Configaturan: datasync-task-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS DataSync tugas telah mengaktifkan pencatatan. Kontrol gagal jika tugas tidak mengaktifkan logging.

Log audit melacak dan memantau aktivitas sistem. Mereka menyediakan catatan peristiwa yang dapat membantu Anda mendeteksi pelanggaran keamanan, menyelidiki insiden, dan mematuhi peraturan. Log audit juga meningkatkan akuntabilitas dan transparansi organisasi Anda secara keseluruhan.

Remediasi

Untuk informasi tentang mengonfigurasi pencatatan AWS DataSync tugas, lihat Memantau transfer data dengan CloudWatch Log Amazon di Panduan AWS DataSync Pengguna.

[DataSync.2] DataSync tugas harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DataSync::Task`

AWS Configaturan: datasync-task-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS DataSync tugas memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika tugas tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai

apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tugas tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS DataSync tugas, lihat Menandai AWS DataSync tugas Anda di Panduan AWS DataSync Pengguna.

Kontrol CSPM Security Hub untuk Amazon Detective

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Detektif Amazon. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Detective.1] Grafik perilaku Detektif harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Detective::Graph`

AWS Configaturan: `tagged-detective-graph` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah grafik perilaku Detektif Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grafik perilaku tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grafik perilaku tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grafik perilaku Detektif, lihat Menambahkan tag ke grafik perilaku di Panduan Administrasi Detektif Amazon.

Kontrol CSPM Security Hub untuk Amazon DocumentDB

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon DocumentDB (dengan kompatibilitas MongoDB). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: docdb-cluster-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon DocumentDB dienkripsi saat istirahat. Kontrol gagal jika cluster Amazon DocumentDB tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah mendapatkan akses ke sana. Data di cluster Amazon DocumentDB harus dienkripsi saat istirahat untuk lapisan keamanan tambahan. Amazon DocumentDB menggunakan Advanced Encryption Standard AES-256 () 256-bit untuk

mengenkripsi data Anda menggunakan kunci enkripsi yang disimpan di (). AWS Key Management Service AWS KMS

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat membuat cluster Amazon DocumentDB. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat Mengaktifkan enkripsi saat istirahat untuk klaster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB.

[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai

Persyaratan terkait: NIST.800-53.r5 SI-12, PCI DSS v4.0. 1/3.2.1

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: docdb-cluster-backup-retention-check

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub	
`minimumBackupRetentionPeriod`	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah klaster Amazon DocumentDB memiliki periode retensi cadangan yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika periode

retensi cadangan kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi cadangan, Security Hub CSPM menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Dengan mengotomatiskan backup untuk cluster Amazon DocumentDB Anda, Anda akan dapat memulihkan sistem Anda ke titik waktu tertentu dan meminimalkan waktu henti dan kehilangan data. Di Amazon DocumentDB, cluster memiliki periode retensi cadangan default 1 hari. Ini harus ditingkatkan menjadi nilai antara 7 dan 35 hari untuk melewati kontrol ini.

Remediasi

Untuk mengubah periode retensi cadangan untuk klaster Amazon DocumentDB Anda, lihat Memodifikasi klaster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB. Untuk Backup, pilih periode retensi cadangan.

[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`

AWS Configaturan: docdb-cluster-snapshot-public-prohibited

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot cluster manual Amazon DocumentDB bersifat publik. Kontrol gagal jika snapshot cluster manual bersifat publik.

Snapshot kluster manual Amazon DocumentDB tidak boleh bersifat publik kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, snapshot tersedia untuk semua. Akun AWS Cuplikan publik dapat mengakibatkan eksposur data yang tidak diinginkan.

> **Note**
>
> Kontrol ini mengevaluasi snapshot cluster manual. Anda tidak dapat membagikan snapshot klaster otomatis Amazon DocumentDB. Namun, Anda dapat membuat snapshot manual dengan menyalin snapshot otomatis, lalu membagikan salinannya.

Remediasi

Untuk menghapus akses publik untuk snapshot kluster manual Amazon DocumentDB, lihat Berbagi snapshot di Panduan Pengembang Amazon DocumentDB. Secara terprogram, Anda dapat menggunakan operasi Amazon DocumentDB. `modify-db-snapshot-attribute` Tetapkan `attribute-name` sebagai `restore` dan `values-to-remove` sebagai`all`.

[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.3.3

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: docdb-cluster-audit-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DocumentDB menerbitkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika klaster tidak mempublikasikan log audit ke CloudWatch Log.

Amazon DocumentDB (dengan kompatibilitas MongoDB) memungkinkan Anda mengaudit peristiwa yang dilakukan di cluster Anda. Contoh log acara termasuk upaya autentikasi yang berhasil dan gagal, membuang koleksi dalam basis data, atau membuat indeks. Secara default, audit dinonaktifkan di Amazon DocumentDB dan mengharuskan Anda mengambil tindakan untuk mengaktifkannya.

Remediasi

Untuk mempublikasikan log audit Amazon DocumentDB CloudWatch ke Log, lihat Mengaktifkan audit di Panduan Pengembang Amazon DocumentDB.

[DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: docdb-cluster-deletion-protection-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DocumentDB mengaktifkan perlindungan penghapusan. Kontrol gagal jika cluster tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan klaster menawarkan lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh pengguna yang tidak sah. Cluster Amazon DocumentDB tidak dapat dihapus saat perlindungan penghapusan diaktifkan. Anda harus menonaktifkan perlindungan penghapusan terlebih dahulu sebelum permintaan penghapusan berhasil. Perlindungan penghapusan diaktifkan secara default saat Anda membuat klaster di konsol Amazon DocumentDB.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster Amazon DocumentDB yang ada, lihat Memodifikasi klaster Amazon DocumentDB di Panduan Pengembang Amazon DocumentDB. Di bagian Modify Cluster, pilih Enable for Deletion protection.

[DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: docdb-cluster-encrypted-in-transit

Jenis jadwal: Periodik

Parameter:`excludeTlsParameters`:`disabled`, `enabled` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah klaster Amazon DocumentDB memerlukan TLS untuk koneksi ke cluster. Kontrol gagal jika grup parameter cluster yang terkait dengan cluster tidak sinkron, atau parameter cluster TLS diatur ke `disabled` atau`enabled`.

Anda dapat menggunakan TLS untuk mengenkripsi koneksi antara aplikasi dan cluster Amazon DocumentDB. Penggunaan TLS dapat membantu melindungi data agar tidak dicegat saat data sedang transit antara aplikasi dan cluster Amazon DocumentDB. Enkripsi dalam perjalanan untuk klaster Amazon DocumentDB dikelola menggunakan parameter TLS di grup parameter cluster yang terkait dengan cluster. Ketika enkripsi dalam transit diaktifkan, koneksi aman menggunakan TLS diperlukan untuk terhubung ke klaster. Sebaiknya gunakan parameter TLS berikut:`tls1.2+`,`tls1.3+`, dan`fips-140-3`.

Remediasi

Untuk informasi tentang mengubah setelan TLS untuk klaster Amazon DocumentDB, lihat Mengenkripsi data saat transit di Panduan Pengembang Amazon DocumentDB.

Kontrol CSPM Security Hub untuk DynamoDB

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon DynamoDB. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[DynamoDB.1] Tabel DynamoDB harus secara otomatis menskalakan kapasitas dengan permintaan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Configaturan: **dynamodb-autoscaling-enabled**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang valid	Nilai default CSPM Security Hub
`minProvisionedReadCapacity`	Jumlah minimum unit kapasitas baca yang disediakan untuk penskalaan otomatis DynamoDB	Bilangan Bulat	1 untuk `40000`	Tidak ada nilai default
`targetReadUtilization`	Target persentase pemanfaatan untuk kapasitas baca	Bilangan Bulat	`20` untuk `90`	Tidak ada nilai default
`minProvisionedWriteCapacity`	Jumlah minimum unit kapasitas tulis yang disediakan untuk penskalaan otomatis DynamoDB	Bilangan Bulat	1 untuk `40000`	Tidak ada nilai default
`targetWriteUtilization`	Target persentase pemanfaatan untuk kapasitas tulis	Bilangan Bulat	`20` untuk `90`	Tidak ada nilai default

Kontrol ini memeriksa apakah tabel Amazon DynamoDB dapat menskalakan kapasitas baca dan tulisnya sesuai kebutuhan. Kontrol gagal jika tabel tidak menggunakan mode kapasitas sesuai permintaan atau mode yang disediakan dengan penskalaan otomatis yang dikonfigurasi. Secara default, kontrol ini hanya mengharuskan salah satu mode ini dikonfigurasi, tanpa memperhatikan tingkat kapasitas baca atau tulis tertentu. Secara opsional, Anda dapat memberikan nilai parameter khusus untuk memerlukan tingkat kapasitas baca dan tulis tertentu atau pemanfaatan target.

Kapasitas penskalaan dengan permintaan menghindari pengecualian pembatasan, yang membantu menjaga ketersediaan aplikasi Anda. Tabel DynamoDB yang menggunakan mode kapasitas sesuai permintaan hanya dibatasi oleh kuota tabel default throughput DynamoDB. Untuk menaikkan kuota

ini, Anda dapat mengajukan tiket dukungan denganDukungan. Tabel DynamoDB yang menggunakan mode yang disediakan dengan penskalaan otomatis menyesuaikan kapasitas throughput yang disediakan secara dinamis sebagai respons terhadap pola lalu lintas. Untuk informasi selengkapnya tentang pembatasan permintaan DynamoDB, lihat Meminta pelambatan dan kapasitas burst di Panduan Pengembang Amazon DynamoDB.

Remediasi

Untuk mengaktifkan penskalaan otomatis DynamoDB pada tabel yang ada dalam mode kapasitas, lihat Mengaktifkan penskalaan otomatis DynamoDB pada tabel yang ada di Panduan Pengembang Amazon DynamoDB.

[DynamoDB.2] Tabel DynamoDB harus mengaktifkan pemulihan point-in-time

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Configaturan: **`dynamodb-pitr-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemulihan point-in-time (PITR) diaktifkan untuk tabel Amazon DynamoDB.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. DynamoDB point-in-time recovery mengotomatiskan backup untuk tabel DynamoDB. Ini mengurangi waktu untuk memulihkan dari menghapus atau menulis operasi yang tidak disengaja. Tabel DynamoDB yang mengaktifkan PITR dapat dikembalikan ke titik waktu mana pun dalam 35 hari terakhir.

Remediasi

Untuk mengembalikan tabel DynamoDB ke titik waktu, lihat Memulihkan tabel DynamoDB ke titik waktu dalam Panduan Pengembang Amazon DynamoDB.

[DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DAX::Cluster`

AWS Configaturan: **`dax-encryption-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DynamoDB Accelerator (DAX) dienkripsi saat istirahat. Kontrol gagal jika cluster DAX tidak dienkripsi saat istirahat.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk yang diakses oleh pengguna yang tidak diautentikasi. AWS Enkripsi menambahkan satu set kontrol akses lain untuk membatasi kemampuan pengguna yang tidak sah untuk mengakses data. Misalnya, izin API diperlukan untuk mendekripsi data sebelum dapat dibaca.

Remediasi

Anda tidak dapat mengaktifkan atau menonaktifkan enkripsi saat istirahat setelah cluster dibuat. Anda harus membuat ulang cluster untuk mengaktifkan enkripsi saat istirahat. Untuk petunjuk terperinci tentang cara membuat klaster DAX dengan enkripsi saat istirahat diaktifkan, lihat Mengaktifkan enkripsi saat istirahat menggunakan Panduan Pengembang Amazon DynamoDB Konsol Manajemen AWS di Amazon DynamoDB.

[DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Configaturan: **`dynamodb-resources-protected-by-backup-plan`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`backupVaultLockCheck`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke `true` dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	`true` atau `false`	Tidak ada nilai default

Kontrol ini mengevaluasi apakah `ACTIVE` tabel Amazon DynamoDB dalam status dicakup oleh rencana cadangan. Kontrol gagal jika tabel DynamoDB tidak dicakup oleh rencana cadangan. Jika Anda menyetel `backupVaultLockCheck` parameter sama dengan`true`, kontrol hanya akan diteruskan jika tabel DynamoDB dicadangkan di AWS Backup vault terkunci.

AWS Backupadalah layanan pencadangan yang dikelola sepenuhnya yang membantu Anda memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS DenganAWS Backup, Anda dapat membuat rencana cadangan yang menentukan persyaratan pencadangan Anda, seperti seberapa sering mencadangkan data Anda dan berapa lama untuk menyimpan cadangan tersebut. Menyertakan tabel DynamoDB dalam paket cadangan membantu Anda melindungi data dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan tabel DynamoDB ke AWS Backup paket cadangan, lihat Menetapkan sumber daya ke paket cadangan di Panduan Pengembang. AWS Backup

[DynamoDB.5] Tabel DynamoDB harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Configaturan: `tagged-dynamodb-table` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah tabel Amazon DynamoDB memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tabel tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tabel DynamoDB, lihat Menandai sumber daya di DynamoDB di Panduan Pengembang Amazon DynamoDB.

[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DynamoDB::Table`

AWS Configaturan: **`dynamodb-table-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah tabel Amazon DynamoDB memiliki perlindungan penghapusan yang diaktifkan. Kontrol gagal jika tabel DynamoDB tidak mengaktifkan proteksi penghapusan.

Anda dapat melindungi tabel DynamoDB dari penghapusan yang tidak disengaja dengan properti perlindungan penghapusan. Mengaktifkan properti ini untuk tabel membantu memastikan bahwa tabel tidak terhapus secara tidak sengaja selama operasi manajemen tabel reguler oleh administrator Anda. Ini membantu mencegah gangguan pada operasi bisnis normal Anda.

Remediasi

Untuk mengaktifkan perlindungan penghapusan untuk tabel DynamoDB, lihat Menggunakan perlindungan penghapusan di Panduan Pengembang Amazon DynamoDB.

[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit

Persyaratan terkait: NIST.800-53.r5 AC-17,, NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::DAX::Cluster`

AWS Configaturan: **`dax-tls-endpoint-encryption`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon DynamoDB Accelerator (DAX) dienkripsi saat transit, dengan jenis enkripsi endpoint disetel ke TLS. Kontrol gagal jika klaster DAX tidak dienkripsi saat transit.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan serangan person-in-the-middle atau serupa untuk menguping atau memanipulasi lalu lintas jaringan. Anda hanya boleh mengizinkan koneksi terenkripsi melalui TLS untuk mengakses kluster DAX. Namun, mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan enkripsi diaktifkan untuk memahami profil kinerja dan dampak TLS.

Remediasi

Anda tidak dapat mengubah setelan enkripsi TLS setelah membuat cluster DAX. Untuk mengenkripsi klaster DAX yang ada, buat klaster baru dengan enkripsi saat transit diaktifkan, geser lalu lintas aplikasi Anda ke klaster tersebut, lalu hapus klaster lama. Untuk informasi selengkapnya, lihat Menggunakan perlindungan penghapusan di Panduan Pengembang Amazon DynamoDB.

Kontrol CSPM Security Hub untuk Amazon EC2

AWS Security Hub CSPM Kontrol ini mengevaluasi layanan dan sumber daya Amazon Elastic Compute Cloud (Amazon EC2). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EC2.1] Snapshot Amazon EBS tidak boleh dikonfigurasi agar dapat dipulihkan secara publik

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`ebs-snapshot-public-restorable-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot Amazon Elastic Block Store dikonfigurasi agar dapat dipulihkan secara publik. Kontrol gagal jika snapshot Amazon EBS dikonfigurasi agar dapat dipulihkan oleh semua.

Snapshot EBS digunakan untuk mencadangkan data pada volume EBS Anda ke Amazon S3 pada titik waktu tertentu. Anda dapat menggunakan snapshot untuk memulihkan status volume EBS sebelumnya. Jarang dapat diterima untuk berbagi snapshot dengan publik. Biasanya keputusan untuk membagikan snapshot secara publik dibuat karena kesalahan atau tanpa pemahaman lengkap tentang implikasinya. Pemeriksaan ini membantu memastikan bahwa semua pembagian tersebut sepenuhnya direncanakan dan disengaja.

Remediasi

Untuk menjadikan snapshot EBS publik menjadi pribadi, lihat Membagikan snapshot di Panduan Pengguna Amazon EC2. Untuk Tindakan, Ubah izin, pilih Pribadi.

[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/5.5, PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/2.1, Tolok Ukur Yayasan AWS CIS v1.2. 0/4.3, Tolok Ukur Yayasan AWS CIS v1.4. 0/5.3, Tolok Ukur Yayasan AWS CIS v3.0. 0/5.4, NIST.800-53.r5 AC-4,

NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-default-security-group-closed`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan default VPC memungkinkan lalu lintas masuk atau keluar. Kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk atau keluar.

Aturan untuk grup keamanan default memungkinkan semua lalu lintas keluar dan masuk dari antarmuka jaringan (dan instance terkait) yang ditetapkan ke grup keamanan yang sama. Kami menyarankan Anda untuk tidak menggunakan grup keamanan default. Karena grup keamanan default tidak dapat dihapus, Anda harus mengubah pengaturan aturan grup keamanan default untuk membatasi lalu lintas masuk dan keluar. Ini mencegah lalu lintas yang tidak diinginkan jika grup keamanan default secara tidak sengaja dikonfigurasi untuk sumber daya seperti instans EC2.

Remediasi

Untuk mengatasi masalah ini, mulailah dengan membuat grup keamanan paling tidak memiliki hak istimewa baru. Untuk petunjuknya, lihat Membuat grup keamanan di Panduan Pengguna Amazon VPC. Kemudian, tetapkan grup keamanan baru ke instans EC2 Anda. Untuk petunjuknya, lihat Mengubah grup keamanan instans di Panduan Pengguna Amazon EC2.

Setelah Anda menetapkan grup keamanan baru ke sumber daya Anda, hapus semua aturan masuk dan keluar dari grup keamanan default. Untuk petunjuknya, lihat Mengonfigurasi aturan grup keamanan di Panduan Pengguna Amazon VPC.

[EC2.3] Volume Amazon EBS yang terlampir harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Volume`

AWS Config aturan: **`encrypted-volumes`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah volume EBS yang berada dalam keadaan terlampir dienkripsi. Untuk lulus pemeriksaan ini, volume EBS harus digunakan dan dienkripsi. Jika volume EBS tidak terpasang, maka tidak tunduk pada pemeriksaan ini.

Untuk lapisan keamanan tambahan data sensitif Anda dalam volume EBS, Anda harus mengaktifkan enkripsi EBS saat istirahat. Enkripsi Amazon EBS menawarkan solusi enkripsi langsung untuk sumber daya EBS Anda yang tidak mengharuskan Anda membangun, memelihara, dan mengamankan infrastruktur manajemen kunci Anda sendiri. Ini menggunakan kunci KMS saat membuat volume dan snapshot terenkripsi.

Untuk mempelajari lebih lanjut tentang enkripsi Amazon EBS, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EC2.

Remediasi

Tidak ada cara langsung untuk mengenkripsi volume atau snapshot yang tidak terenkripsi yang ada. Anda hanya dapat mengenkripsi volume atau snapshot baru saat Anda membuatnya.

Jika Anda mengaktifkan enkripsi secara default, Amazon EBS mengenkripsi volume atau snapshot baru yang dihasilkan menggunakan kunci default untuk enkripsi Amazon EBS. Meskipun Anda belum mengaktifkan enkripsi secara default, Anda dapat mengaktifkan enkripsi saat Anda membuat volume atau snapshot individu. Dalam kedua kasus tersebut, Anda dapat mengganti kunci default untuk enkripsi Amazon EBS dan memilih kunci terkelola pelanggan simetris.

Untuk informasi selengkapnya, lihat Membuat volume Amazon EBS dan Menyalin snapshot Amazon EBS di Panduan Pengguna Amazon EC2.

[EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: `ec2-stopped-instance-days-check` (aturan CSPM Security Hub kustom)

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`AllowedDays`	Jumlah hari instans EC2 diizinkan berada dalam keadaan berhenti sebelum menghasilkan temuan yang gagal.	Bilangan Bulat	1 untuk `365`	`30`

Kontrol ini memeriksa apakah instans Amazon EC2 telah dihentikan lebih lama dari jumlah hari yang diizinkan. Kontrol gagal jika instans EC2 dihentikan lebih lama dari periode waktu maksimum yang diizinkan. Kecuali Anda memberikan nilai parameter khusus untuk jangka waktu maksimum yang diizinkan, Security Hub CSPM menggunakan nilai default 30 hari.

Ketika instans EC2 tidak berjalan untuk jangka waktu yang signifikan, itu menciptakan risiko keamanan karena instans tidak dipelihara secara aktif (dianalisis, ditambal, diperbarui). Jika kemudian diluncurkan, kurangnya perawatan yang tepat dapat mengakibatkan masalah tak terduga di AWS lingkungan Anda. Untuk mempertahankan instans EC2 dengan aman dari waktu ke waktu dalam keadaan tidak aktif, mulailah secara berkala untuk pemeliharaan dan kemudian hentikan setelah pemeliharaan. Idealnya, ini harus menjadi proses otomatis.

> **Note**
>
> Kontrol ini mengevaluasi jumlah hari dimana instans EC2 telah dihentikan menggunakan stempel waktu dari `StateTransitionReason` instance. Ketika `StateTransitionReason` tidak menyertakan stempel waktu (seperti ketika instance dihentikan karena kesalahan internal), kontrol menggunakan waktu peluncuran instance sebagai gantinya. Dalam hal

ini, jika waktu peluncuran lebih tua dari periode waktu maksimum yang diizinkan, kontrol menghasilkan temuan GAGAL.

Remediasi

Untuk menghentikan instans EC2 yang tidak aktif, lihat Mengakhiri instance di Panduan Pengguna Amazon EC2.

[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/3.7, Tolok Ukur Yayasan AWS CIS v1.2. 0/2.9, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.9, Tolok Ukur Yayasan AWS CIS v3.0. 0/3.7, NIST.800-53.r5 AC-4 (26),,, NIST.800-53.r5 AU-12 NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-3, (4),, NIST.800-53.r5 AU-6 NIST.800-53.r5 SI-7 (8) NIST.800-53.r5 CA-7, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, PCI DSS v3.2. 1/10.3.3, PCI DSS v3.2. 1/10.3.4, PCI DSS v3.2. 1/10.3.5, PCI DSS v3.2. 1/10.3.6

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPC`

AWS Config aturan: **`vpc-flow-logs-enabled`**

Jenis jadwal: Periodik

Parameter:

- `trafficType`: `REJECT` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Amazon VPC Flow Logs ditemukan dan diaktifkan untuk VPC. Jenis lalu lintas diatur ke`Reject`. Kontrol gagal jika VPC Flow Logs tidak diaktifkan untuk VPC di akun Anda.

> **Note**
>
> Kontrol ini tidak memeriksa apakah Amazon VPC Flow Logs diaktifkan melalui Amazon Security Lake untuk file. Akun AWS

Dengan fitur VPC Flow Logs, Anda dapat menangkap informasi tentang lalu lintas alamat IP yang menuju dan dari antarmuka jaringan di VPC Anda. Setelah membuat log aliran, Anda dapat melihat dan mengambil datanya di CloudWatch Log. Untuk mengurangi biaya, Anda juga dapat mengirim log aliran Anda ke Amazon S3.

Security Hub CSPM merekomendasikan agar Anda mengaktifkan flow logging untuk penolakan paket untuk VPC. Flow log memberikan visibilitas ke lalu lintas jaringan yang melintasi VPC dan dapat mendeteksi lalu lintas anomali atau memberikan wawasan selama alur kerja keamanan.

Secara default, catatan menyertakan nilai untuk berbagai komponen aliran alamat IP, termasuk sumber, tujuan, dan protokol. Untuk informasi selengkapnya dan deskripsi bidang log, lihat Log Aliran VPC di Panduan Pengguna Amazon VPC.

Remediasi

Untuk membuat Log Aliran VPC, lihat Membuat Log Aliran di Panduan Pengguna Amazon VPC. Setelah Anda membuka konsol VPC Amazon, pilih VPC Anda. Untuk Filter, pilih Tolak atau Semua.

[EC2.7] Enkripsi default EBS harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/5.1.1, Tolok Ukur Yayasan AWS CIS v1.4. 0/2.2.1, Tolok Ukur Yayasan AWS CIS v3.0. 0/2.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: **`ec2-ebs-encryption-by-default`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah enkripsi tingkat akun diaktifkan secara default untuk volume Amazon Elastic Block Store (Amazon EBS). Kontrol gagal jika enkripsi tingkat akun tidak diaktifkan untuk volume EBS.

Saat enkripsi diaktifkan untuk akun Anda, volume Amazon EBS dan salinan snapshot dienkripsi saat istirahat. Ini menambahkan lapisan perlindungan tambahan untuk data Anda. Untuk informasi selengkapnya, lihat Enkripsi secara default di Panduan Pengguna Amazon EC2.

Remediasi

Untuk mengonfigurasi enkripsi default untuk volume Amazon EBS, lihat Enkripsi secara default di Panduan Pengguna Amazon EC2.

[EC2.8] Instans EC2 harus menggunakan Layanan Metadata Instance Versi 2 (IMDSv2)

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/5.7, Tolok Ukur Yayasan AWS CIS v3.0. 0/5.6, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/2.2.6

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-imdsv2-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah versi metadata instans EC2 Anda dikonfigurasi dengan Instance Metadata Service Version 2 (IMDSv2). Kontrol lolos jika `HttpTokens` disetel ke required untuk IMDSv2. Kontrol gagal jika `HttpTokens` diatur ke`optional`.

Anda menggunakan metadata instance untuk mengonfigurasi atau mengelola instance yang sedang berjalan. IMDS menyediakan akses ke kredensil sementara yang sering diputar. Kredensyal ini menghapus kebutuhan untuk kode keras atau mendistribusikan kredensyal sensitif ke instance secara manual atau terprogram. IMDS dilampirkan secara lokal ke setiap instans EC2. Ini berjalan pada alamat IP “link lokal” khusus 169.254.169.254. Alamat IP ini hanya dapat diakses oleh perangkat lunak yang berjalan pada instance.

Versi 2 IMDS menambahkan perlindungan baru untuk jenis kerentanan berikut. Kerentanan ini dapat digunakan untuk mencoba mengakses IMDS.

- Buka firewall aplikasi situs web
- Buka proxy terbalik

- Server-side kerentanan permintaan pemalsuan (SSRF)
- Buka firewall Layer 3 dan terjemahan alamat jaringan (NAT)

Security Hub CSPM merekomendasikan agar Anda mengonfigurasi instans EC2 Anda dengan IMDSv2.

Remediasi

Untuk mengonfigurasi instans EC2 dengan IMDSv2, lihat Jalur yang disarankan untuk mewajibkan IMDSv2 di Panduan Pengguna Amazon EC2.

[EC2.9] Instans Amazon EC2 seharusnya tidak memiliki alamat IPv4 publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-instance-no-public-ip`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans EC2 memiliki alamat IP publik. Kontrol gagal jika `publicIp` bidang hadir dalam item konfigurasi instans EC2. Kontrol ini hanya berlaku untuk alamat IPv4.

Alamat IPv4 publik adalah alamat IP yang dapat dijangkau dari internet. Jika Anda meluncurkan instans Anda dengan alamat IP publik, maka instans EC2 Anda dapat dijangkau dari internet. Alamat IPv4 pribadi adalah alamat IP yang tidak dapat dijangkau dari internet. Anda dapat menggunakan alamat IPv4 pribadi untuk komunikasi antara instans EC2 di VPC yang sama atau di jaringan pribadi Anda yang terhubung.

Alamat IPv6 unik secara global, dan karenanya dapat dijangkau dari internet. Namun, secara default semua subnet memiliki atribut pengalamatan IPv6 disetel ke false. Untuk informasi selengkapnya tentang IPv6, lihat Pengalamatan IP di VPC Anda di Panduan Pengguna Amazon VPC.

Jika Anda memiliki kasus penggunaan yang sah untuk mempertahankan instans EC2 dengan alamat IP publik, maka Anda dapat menekan temuan dari kontrol ini. Untuk informasi selengkapnya tentang opsi arsitektur front-end, lihat Blog AWS Arsitektur atau seri AWS video seri This Is My Architecture.

Remediasi

Gunakan VPC non-default sehingga instans Anda tidak diberi alamat IP publik secara default.

Ketika Anda meluncurkan instans EC2 ke VPC default, itu diberikan alamat IP publik. Saat Anda meluncurkan instans EC2 ke VPC non-default, konfigurasi subnet menentukan apakah ia menerima alamat IP publik. Subnet memiliki atribut untuk menentukan apakah instans EC2 baru di subnet menerima alamat IP publik dari kumpulan alamat IPv4 publik.

Anda dapat memisahkan alamat IP publik yang ditetapkan secara otomatis dari instans EC2 Anda. Untuk informasi selengkapnya, lihat Alamat IPv4 publik dan nama host DNS eksternal di Panduan Pengguna Amazon EC2.

[EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1

Kategori: Lindungi > Konfigurasi jaringan aman > Akses pribadi API

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPC`

AWS Config aturan: vpc-endpoint-enabled

Jenis jadwal: Periodik

Parameter:

- `serviceNames`: `ec2` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah titik akhir layanan untuk Amazon EC2 dibuat untuk setiap VPC. Kontrol gagal jika VPC tidak memiliki titik akhir VPC yang dibuat untuk layanan Amazon EC2.

Kontrol ini mengevaluasi sumber daya dalam satu akun. Itu tidak dapat menggambarkan sumber daya yang berada di luar akun. Karena AWS Config dan Security Hub CSPM tidak melakukan pemeriksaan lintas akun, Anda akan melihat `FAILED` temuan untuk VPC yang dibagikan di seluruh akun. Security Hub CSPM merekomendasikan agar Anda menekan temuan ini. `FAILED`

Untuk meningkatkan postur keamanan VPC Anda, Anda dapat mengonfigurasi Amazon EC2 untuk menggunakan titik akhir VPC antarmuka. Endpoint antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses operasi Amazon EC2 API secara pribadi. Ini membatasi semua lalu lintas jaringan antara VPC Anda dan Amazon EC2 ke jaringan Amazon. Karena titik akhir hanya didukung dalam Wilayah yang sama, Anda tidak dapat membuat titik akhir antara VPC dan layanan di Wilayah yang berbeda. Ini mencegah panggilan API Amazon EC2 yang tidak diinginkan ke Wilayah lain.

Untuk mempelajari selengkapnya tentang membuat titik akhir VPC untuk Amazon EC2, lihat Amazon EC2 dan titik akhir VPC antarmuka di Panduan Pengguna Amazon EC2.

Remediasi

Untuk membuat titik akhir antarmuka ke Amazon EC2 dari konsol VPC Amazon, lihat Membuat titik akhir VPC di Panduan.AWS PrivateLink Untuk nama Layanan, pilih com.amazonaws. ***region***.ec2.

Anda juga dapat membuat dan melampirkan kebijakan titik akhir ke titik akhir VPC Anda untuk mengontrol akses ke Amazon EC2 API. Untuk petunjuk cara membuat kebijakan titik akhir VPC, lihat Membuat kebijakan titik akhir di Panduan Pengguna Amazon EC2.

[EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus

Persyaratan terkait: PCI DSS v3.2. 1/2.4, NIST.800-53.r5 CM-8 (1)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::EIP`

AWS Config aturan: **`eip-attached`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah alamat Elastic IP (EIP) yang dialokasikan ke VPC dilampirkan ke instans EC2 atau antarmuka jaringan elastis (ENI) yang sedang digunakan.

Temuan yang gagal menunjukkan Anda mungkin memiliki EC2 EIP yang tidak digunakan.

Ini akan membantu Anda mempertahankan inventaris aset EIP yang akurat di lingkungan data pemegang kartu (CDE) Anda.

Remediasi

Untuk merilis EIP yang tidak digunakan, lihat Melepaskan alamat IP Elastis di Panduan Pengguna Amazon EC2.

[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/4.1, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1, PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/2.2.2, PCI DSS v4.0. 1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`restricted-ssh`**

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memungkinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22. Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0. 0/0atau: :/0 ke port 22.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port 22. Menghapus konektivitas tanpa batas ke layanan konsol jarak jauh, seperti SSH, mengurangi eksposur server terhadap risiko.

Remediasi

Untuk melarang masuknya ke port 22, hapus aturan yang memungkinkan akses tersebut untuk setiap grup keamanan yang terkait dengan VPC. Untuk petunjuknya, lihat Memperbarui aturan grup

keamanan di Panduan Pengguna Amazon EC2. Setelah memilih grup keamanan di konsol Amazon EC2, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22.

[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/4.2, PCI DSS v4.0. 1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`restricted-common-ports`**(aturan yang dibuat adalah`restricted-rdp`)

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memungkinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389. Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0. 0/0atau: :/0 ke port 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port 3389. Menghapus konektivitas tanpa batas ke layanan konsol jarak jauh, seperti RDP, mengurangi eksposur server terhadap risiko.

Remediasi

Untuk melarang masuknya ke port 3389, hapus aturan yang memungkinkan akses tersebut untuk setiap grup keamanan yang terkait dengan VPC. Untuk petunjuknya, lihat Memperbarui aturan grup keamanan di Panduan Pengguna Amazon VPC. Setelah memilih grup keamanan di Konsol VPC Amazon, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 3389.

[EC2.15] Subnet Amazon EC2 seharusnya tidak secara otomatis menetapkan alamat IP publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Subnet`

AWS Config aturan: **`subnet-auto-assign-public-ip-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah subnet Amazon Virtual Private Cloud (Amazon VPC) dikonfigurasi untuk secara otomatis menetapkan alamat IP publik. Kontrol gagal jika subnet dikonfigurasi untuk secara otomatis menetapkan alamat IPv4 atau IPv6 publik.

Subnet memiliki atribut yang menentukan apakah antarmuka jaringan secara otomatis menerima alamat IPv4 dan IPv6 publik. Untuk IPv4, atribut ini disetel ke subnet default dan `TRUE` `FALSE` untuk subnet nondefault (dengan pengecualian untuk subnet nondefault yang dibuat melalui wizard instans peluncuran EC2, yang disetel ke). `TRUE` Untuk IPv6, atribut ini diatur `FALSE` untuk semua subnet secara default. Ketika atribut ini diaktifkan, instance yang diluncurkan di subnet secara otomatis menerima alamat IP yang sesuai (IPv4 atau IPv6) pada antarmuka jaringan utama mereka.

Remediasi

Untuk mengonfigurasi subnet agar tidak menetapkan alamat IP publik, lihat Memodifikasi atribut pengalamatan IP subnet Anda di Panduan Pengguna Amazon VPC.

[EC2.16] Daftar Kontrol Akses Jaringan yang Tidak Digunakan harus dihapus

Persyaratan terkait: NIST.800-53.r5 CM-8 (1), NIST.800-171.r2 3.4.7, PCI DSS v4.0. 1/1.2.7

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkAcl`

AWS Config aturan: **`vpc-network-acl-unused-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ada daftar kontrol akses jaringan (ACL jaringan) yang tidak digunakan di cloud pribadi virtual (VPC) Anda. Kontrol gagal jika ACL jaringan tidak terkait dengan subnet. Kontrol tidak menghasilkan temuan untuk ACL jaringan default yang tidak digunakan.

Kontrol memeriksa konfigurasi item sumber daya `AWS::EC2::NetworkAcl` dan menentukan hubungan ACL jaringan.

Jika satu-satunya hubungan adalah VPC jaringan ACL, kontrol gagal.

Jika hubungan lain terdaftar, maka kontrol berlalu.

Remediasi

Untuk petunjuk cara menghapus ACL jaringan yang tidak digunakan, lihat Menghapus ACL jaringan di Panduan Pengguna Amazon VPC. Anda tidak dapat menghapus ACL jaringan default atau ACL yang terkait dengan subnet.

[EC2.17] Instans Amazon EC2 tidak boleh menggunakan beberapa ENI

Persyaratan terkait: NIST.800-53.r5 AC-4 (21)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-instance-multiple-eni-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans EC2 menggunakan beberapa Elastic Network Interfaces (ENIs) atau Elastic Fabric Adapters (EFA). Kontrol ini lolos jika adaptor jaringan tunggal digunakan. Kontrol mencakup daftar parameter opsional untuk mengidentifikasi ENI yang diizinkan. Kontrol ini juga gagal jika instans EC2 milik kluster Amazon EKS menggunakan lebih dari satu ENI. Jika instans EC2 Anda perlu memiliki beberapa ENI sebagai bagian dari kluster Amazon EKS, Anda dapat menekan temuan kontrol tersebut.

Beberapa ENI dapat menyebabkan instance dual-homed, yang berarti instance yang memiliki beberapa subnet. Ini dapat menambah kompleksitas keamanan jaringan dan memperkenalkan jalur dan akses jaringan yang tidak diinginkan.

Remediasi

Untuk melepaskan antarmuka jaringan dari instans EC2, lihat Melepaskan antarmuka jaringan dari instans di Panduan Pengguna Amazon EC2.

[EC2.18] Grup keamanan seharusnya hanya mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, 3.13.1 NIST.800-171.r2

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-sg-open-only-to-authorized-ports`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`authorizedTcpPorts`	Daftar port TCP resmi	IntegerList (minimal 1 item dan maksimal 32 item)	1 untuk 65535	`[80,443]`
`authorizedUdpPorts`	Daftar port UDP resmi	IntegerList (minimal 1 item dan maksimal 32 item)	1 untuk 65535	Tidak ada nilai default

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 mengizinkan lalu lintas masuk yang tidak dibatasi dari port yang tidak sah. Status kontrol ditentukan sebagai berikut:

- Jika Anda menggunakan nilai default untuk`authorizedTcpPorts`, kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk yang tidak dibatasi dari port selain port 80 dan 443.
- Jika Anda memberikan nilai khusus untuk `authorizedTcpPorts` atau`authorizedUdpPorts`, kontrol gagal jika grup keamanan mengizinkan lalu lintas masuk yang tidak dibatasi dari port yang tidak terdaftar.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke. AWS Aturan grup keamanan harus mengikuti prinsip akses yang paling tidak memiliki hak istimewa. Akses tidak terbatas (alamat IP dengan akhiran /0) meningkatkan peluang aktivitas berbahaya seperti peretasan, serangan penolakan layanan, dan hilangnya data. Kecuali port diizinkan secara khusus, port harus menolak akses tidak terbatas.

Remediasi

Untuk mengubah grup keamanan, lihat Bekerja dengan grup keamanan di Panduan Pengguna Amazon VPC.

[EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2),, NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, 3.13.1 NIST.800-171.r2

Kategori: Lindungi > Akses jaringan terbatas

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`restricted-common-ports`**(aturan yang dibuat adalah`vpc-sg-restricted-common-ports`)

Jenis jadwal: Perubahan yang dipicu dan berkala

Parameter: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah lalu lintas masuk yang tidak dibatasi untuk grup keamanan Amazon EC2 dapat diakses ke port tertentu yang dianggap berisiko tinggi. Kontrol ini gagal jika salah satu aturan dalam grup keamanan mengizinkan lalu lintas masuk dari '0.0.0. 0/0' atau ': :/0' ke port tersebut.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Akses tidak terbatas (0.0.0. 0/0) meningkatkan peluang untuk aktivitas berbahaya, seperti peretasan, serangan penolakan layanan, dan hilangnya data. Tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port berikut:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)
- 1433, 1434 (MSSQL)
- 3000 (Go, Node.js, dan kerangka kerja pengembangan web Ruby)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Kerangka pengembangan web Python)
- 5432 (Postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (Dasbor) OpenSearch
- 8080 (proksi)
- 8088 (port HTTP lama)

- 8888 (port HTTP alternatif)
- 9200 atau 9300 () OpenSearch

Remediasi

Untuk menghapus aturan dari grup keamanan, lihat Menghapus aturan dari grup keamanan di Panduan Pengguna Amazon EC2.

[EC2.20] Kedua terowongan VPN untuk AWS Site-to-Site Koneksi VPN harus aktif

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.1.13, 3.1.20 NIST.800-171.r2

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPNConnection`

AWS Config aturan: **`vpc-vpn-2-tunnels-up`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Terowongan VPN adalah tautan terenkripsi tempat data dapat berpindah dari jaringan pelanggan ke atau dari AWS dalam koneksi AWS Site-to-Site VPN. Setiap koneksi VPN mencakup dua terowongan VPN yang dapat Anda gunakan secara bersamaan untuk ketersediaan tinggi. Memastikan bahwa kedua terowongan VPN siap untuk koneksi VPN penting untuk mengonfirmasi koneksi yang aman dan sangat tersedia antara AWS VPC dan jaringan jarak jauh Anda.

Kontrol ini memeriksa apakah kedua terowongan VPN yang disediakan oleh AWS Site-to-Site VPN berada dalam status UP. Kontrol gagal jika salah satu atau kedua terowongan berada dalam status DOWN.

Remediasi

Untuk mengubah opsi terowongan VPN, lihat Memodifikasi opsi terowongan Site-to-Site AWS Site-to-Site VPN di Panduan Pengguna VPN.

[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/5.2, Tolok Ukur Yayasan AWS CIS v1.4. 0/5.1, Tolok Ukur Yayasan AWS CIS v3.0. 0/5.1, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1),, (2) NIST.800-53.r5 CM-2,,, NIST.800-53.r5 CM-2 (21) NIST.800-53.r5 CM-7 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1, PCI DSS v4.0. 1/1.3.1

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::NetworkAcl`

AWS Config aturan: **`nacl-no-unrestricted-ssh-rdp`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah daftar kontrol akses jaringan (ACL jaringan) memungkinkan akses tidak terbatas ke port TCP default untuk SSH/RDP lalu lintas masuk. Kontrol gagal jika entri masuk ACL jaringan memungkinkan blok CIDR sumber '0.0.0. 0/0' atau ': :/0' untuk port TCP 22 atau 3389. Kontrol tidak menghasilkan temuan untuk ACL jaringan default.

Akses ke port administrasi server jarak jauh, seperti port 22 (SSH) dan port 3389 (RDP), tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke sumber daya dalam VPC Anda.

Remediasi

Untuk mengedit aturan lalu lintas ACL jaringan, lihat Bekerja dengan ACL jaringan di Panduan Pengguna Amazon VPC.

[EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

AWS Config aturan: **`ec2-security-group-attached-to-eni-periodic`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) atau ke antarmuka elastic network. Kontrol gagal jika grup keamanan tidak terkait dengan instans Amazon EC2 atau elastic network interface.

> **Important**
>
> Pada tanggal 20 September 2023, Security Hub CSPM menghapus kontrol ini dari standar Praktik Terbaik Keamanan AWS Dasar dan NIST SP 800-53 Revisi 5. Kontrol ini terus menjadi bagian dari standar yang AWS Control Tower dikelola layanan. Kontrol ini menghasilkan temuan yang diteruskan jika grup keamanan dilampirkan ke instans EC2 atau elastic network interface. Namun, untuk kasus penggunaan tertentu, kelompok keamanan yang tidak terikat tidak menimbulkan risiko keamanan. Anda dapat menggunakan kontrol EC2 lain—seperti EC2.2,,, EC2.13 EC2.14 EC2.18, dan EC2.19 —untuk memantau grup keamanan Anda.

Remediasi

Untuk membuat, menetapkan, dan menghapus grup keamanan, lihat Grup keamanan untuk instans EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::TransitGateway`

AWS Config aturan: **`ec2-transit-gateway-auto-vpc-attach-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah gateway transit EC2 secara otomatis menerima lampiran VPC bersama. Kontrol ini gagal untuk gateway transit yang secara otomatis menerima permintaan lampiran VPC bersama.

Menghidupkan `AutoAcceptSharedAttachments` mengonfigurasi gateway transit untuk secara otomatis menerima permintaan lampiran VPC lintas akun apa pun tanpa memverifikasi permintaan atau akun tempat lampiran berasal. Untuk mengikuti praktik otorisasi dan otentikasi terbaik, kami sarankan untuk mematikan fitur ini untuk memastikan bahwa hanya permintaan lampiran VPC resmi yang diterima.

Remediasi

Untuk mengubah gateway transit, lihat Memodifikasi gateway transit di Panduan Pengembang Amazon VPC.

[EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan

Persyaratan terkait: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: **`ec2-paravirtual-instance-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah jenis virtualisasi dari instans EC2 adalah paravirtual. Kontrol gagal jika instans EC2 diatur ke`paravirtual`. `virtualizationType`

Linux Amazon Machine Images (AMI) menggunakan salah satu dari dua jenis virtualisasi: paravirtual (PV) atau hardware virtual machine (HVM). Perbedaan utama antara AMI PV dan HVM adalah caranya melakukan boot dan apakah keduanya dapat memanfaatkan ekstensi perangkat keras khusus (CPU, jaringan, dan penyimpanan) untuk performa yang lebih baik.

Secara historis, tamu PV biasanya memiliki performa yang lebih baik dibandingkan tamu HVM, tetapi karena peningkatan virtualisasi HVM dan ketersediaan driver PV untuk HVM HMI, ini tidak lagi benar. Untuk informasi selengkapnya, lihat jenis virtualisasi AMI Linux di Panduan Pengguna Amazon EC2.

Remediasi

Untuk memperbarui instans EC2 ke jenis instans baru, lihat Mengubah jenis instans di Panduan Pengguna Amazon EC2.

[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::LaunchTemplate`

AWS Config aturan: **`ec2-launch-template-public-ip-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah templat peluncuran Amazon EC2 dikonfigurasi untuk menetapkan alamat IP publik ke antarmuka jaringan saat diluncurkan. Kontrol gagal jika template peluncuran EC2 dikonfigurasi untuk menetapkan alamat IP publik ke antarmuka jaringan atau jika ada setidaknya satu antarmuka jaringan yang memiliki alamat IP publik.

Alamat IP publik adalah alamat yang dapat dijangkau dari internet. Jika Anda mengonfigurasi antarmuka jaringan Anda dengan alamat IP publik, maka sumber daya yang terkait dengan antarmuka jaringan tersebut dapat dijangkau dari internet. Sumber daya EC2 tidak boleh diakses publik karena ini memungkinkan akses yang tidak diinginkan ke beban kerja Anda.

Remediasi

Untuk memperbarui template peluncuran EC2, lihat Mengubah setelan antarmuka jaringan default di Panduan Pengguna Amazon EC2 Auto Scaling.

[EC2.28] Volume EBS harus dicakup oleh rencana cadangan

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Volume`

AWS Config aturan: **`ebs-resources-protected-by-backup-plan`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`backupVaultLockCheck`	Kontrol menghasilkan `PASSED` temuan jika parameter disetel ke `true` dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	`true` atau `false`	Tidak ada nilai default

Kontrol ini mengevaluasi jika volume Amazon EBS dalam `in-use` status dicakup oleh paket cadangan. Kontrol gagal jika volume EBS tidak tercakup oleh paket cadangan. Jika Anda menyetel `backupVaultLockCheck` parameter sama dengan`true`, kontrol hanya akan diteruskan jika volume EBS dicadangkan di brankas yang AWS Backup terkunci.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. Menyertakan volume Amazon EBS dalam paket cadangan membantu Anda melindungi data dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan volume Amazon EBS ke paket AWS Backup cadangan, lihat Menetapkan sumber daya ke paket cadangan di Panduan AWS Backup Pengembang.

[EC2.33] Lampiran gateway transit EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGatewayAttachment`

AWS Config aturan: `tagged-ec2-transitgatewayattachment` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah lampiran gateway transit Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika lampiran gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika lampiran gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke lampiran gateway transit EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.34] Tabel rute gateway transit EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGatewayRouteTable`

AWS Config aturan: `tagged-ec2-transitgatewayroutetable` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah tabel rute gateway transit Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tabel rute gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel rute gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tabel rute gateway transit EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.35] Antarmuka jaringan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkInterface`

AWS Config aturan: `tagged-ec2-networkinterface` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah antarmuka jaringan Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika antarmuka jaringan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antarmuka jaringan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke antarmuka jaringan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.36] Gateway pelanggan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::CustomerGateway`

AWS Config aturan: `tagged-ec2-customergateway` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah gateway pelanggan Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway pelanggan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway pelanggan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway pelanggan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.37] Alamat IP Elastis EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::EIP`

AWS Config aturan: `tagged-ec2-eip` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah alamat IP Elastis Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika alamat IP Elastis tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alamat IP Elastis tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alamat IP Elastis EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.38] Instans EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Instance`

AWS Config aturan: `tagged-ec2-instance` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah instans Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika instance tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instans EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.39] Gerbang internet EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::InternetGateway`

AWS Config aturan: `tagged-ec2-internetgateway` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah gateway internet Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway internet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway internet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway internet EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.40] Gerbang EC2 NAT harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NatGateway`

AWS Config aturan: `tagged-ec2-natgateway` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah gateway terjemahan alamat jaringan (NAT) Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway NAT tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway NAT tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway EC2 NAT, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.41] ACL jaringan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::NetworkAcl`

AWS Config aturan: `tagged-ec2-networkacl` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar kontrol akses jaringan Amazon EC2 (ACL jaringan) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika ACL jaringan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika ACL jaringan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke ACL jaringan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.42] Tabel rute EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::RouteTable`

AWS Config aturan: `tagged-ec2-routetable` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah tabel rute Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tabel rute tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tabel rute tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tabel rute EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.43] Grup keamanan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: `tagged-ec2-securitygroup` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup keamanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup keamanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup keamanan EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.44] Subnet EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Subnet`

AWS Config aturan: `tagged-ec2-subnet` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah subnet Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika subnet tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika subnet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke subnet EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.45] Volume EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::Volume`

AWS Config aturan: `tagged-ec2-volume` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah volume Amazon EC2 memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika volume tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika volume tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke volume EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.46] Amazon VPC harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPC`

AWS Config aturan: `tagged-ec2-vpc` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah Amazon Virtual Private Cloud (Amazon VPC) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika VPC Amazon tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika VPC Amazon tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke VPC, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.47] Layanan titik akhir Amazon VPC harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPCEndpointService`

AWS Config aturan: `tagged-ec2-vpcendpointservice` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah layanan titik akhir VPC Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika layanan endpoint tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika layanan titik akhir tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke layanan titik akhir Amazon VPC, lihat Mengelola Tag di bagian Mengonfigurasi layanan titik akhir dari Panduan.AWS PrivateLink

[EC2.48] Log aliran VPC Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::FlowLog`

AWS Config aturan: `tagged-ec2-flowlog` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah log aliran VPC Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika log aliran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika log aliran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke log aliran VPC Amazon, lihat Menandai log alur di Panduan Pengguna Amazon VPC.

[EC2.49] Koneksi peering VPC Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPCPeeringConnection`

AWS Config aturan: `tagged-ec2-vpcpeeringconnection` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah koneksi peering VPC Amazon memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika koneksi peering tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika koneksi peering tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke koneksi peering VPC Amazon, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.50] Gateway EC2 VPN harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::VPNGateway`

AWS Config aturan: `tagged-ec2-vpngateway` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratan AWS .	

Kontrol ini memeriksa apakah gateway Amazon EC2 VPN memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway VPN tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway VPN tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway VPN EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),,,, NIST.800-53.r5 AU-10 NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-6 (3) NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, (4), NIST.800-53.r5 AU-6 (7),, NIST.800-53.r5 AU-9 (9), NIST.800-53.r5 SC-7 (8) NIST.800-53.r5 CA-7,, NIST.800-53.r5 SI-3 (20), (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.12, NIST.800-171.r2 3.1.20, PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::ClientVpnEndpoint`

AWS Config aturan: **`ec2-client-vpn-connection-log-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Client VPN titik akhir mengaktifkan pencatatan koneksi klien. Kontrol gagal jika titik akhir tidak mengaktifkan pencatatan koneksi klien.

Titik akhir Client VPN memungkinkan klien jarak jauh untuk terhubung dengan aman ke sumber daya di Virtual Private Cloud (VPC) di. AWS Log koneksi memungkinkan Anda melacak aktivitas pengguna di titik akhir VPN dan memberikan visibilitas. Bila Anda mengaktifkan logging koneksi, Anda dapat menentukan nama pengaliran log dalam grup log. Jika Anda tidak menentukan aliran log, layanan Client VPN membuatnya untuk Anda.

Remediasi

Untuk mengaktifkan pencatatan koneksi, lihat Mengaktifkan pencatatan koneksi untuk titik akhir Client VPN yang ada di Panduan AWS Client VPN Administrator.

[EC2.52] Gerbang transit EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TransitGateway`

AWS Config aturan: `tagged-ec2-transitgateway` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	`No default value`

Kontrol ini memeriksa apakah gateway transit Amazon EC2 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika gateway transit tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway transit tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke gateway transit EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/5.3, Tolok Ukur Yayasan AWS CIS v3.0. 0/5.2, PCI DSS v4.0. 1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-sg-port-restriction-check`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`ipType`	Versi IP	String	Tidak dapat disesuaikan	`IPv4`
`restrictPorts`	Daftar port yang harus menolak lalu lintas masuk	IntegerList	Tidak dapat disesuaikan	`22,3389`

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memungkinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh (port 22 dan 3389). Kontrol gagal jika grup keamanan mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port administrasi server jarak jauh, seperti SSH ke port 22 dan RDP ke port 3389, menggunakan protokol TDP (6), UDP (17), atau ALL (-1). Memungkinkan akses publik ke port ini meningkatkan permukaan serangan sumber daya dan risiko kompromi sumber daya.

Remediasi

Untuk memperbarui aturan grup keamanan EC2 untuk melarang lalu lintas masuk ke port yang ditentukan, lihat Memperbarui aturan grup keamanan di Panduan Pengguna Amazon EC2. Setelah memilih grup keamanan di konsol Amazon EC2, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22 atau port 3389.

[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/5.4, Tolok Ukur Yayasan AWS CIS v3.0. 0/5.3, PCI DSS v4.0. 1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SecurityGroup`

AWS Config aturan: **`vpc-sg-port-restriction-check`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`ipType`	Versi IP	String	Tidak dapat disesuaikan	`IPv6`
`restrictPorts`	Daftar port yang harus menolak lalu lintas masuk	IntegerList	Tidak dapat disesuaikan	`22,3389`

Kontrol ini memeriksa apakah grup keamanan Amazon EC2 memungkinkan masuknya dari: :/0 ke port administrasi server jarak jauh (port 22 dan 3389). Kontrol gagal jika grup keamanan mengizinkan masuknya dari: :/0 ke port 22 atau 3389.

Grup keamanan menyediakan penyaringan stateful dari lalu lintas jaringan masuk dan keluar ke sumber daya. AWS Kami menyarankan agar tidak ada grup keamanan yang mengizinkan akses masuk tanpa batas ke port administrasi server jarak jauh, seperti SSH ke port 22 dan RDP ke port 3389, menggunakan protokol TDP (6), UDP (17), atau ALL (-1). Memungkinkan akses publik ke port ini meningkatkan permukaan serangan sumber daya dan risiko kompromi sumber daya.

Remediasi

Untuk memperbarui aturan grup keamanan EC2 untuk melarang lalu lintas masuk ke port yang ditentukan, lihat Memperbarui aturan grup keamanan di Panduan Pengguna Amazon EC2. Setelah memilih grup keamanan di konsol Amazon EC2, pilih Tindakan, Edit aturan masuk. Hapus aturan yang memungkinkan akses ke port 22 atau port 3389.

[EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config aturan: vpc-endpoint-enabled

Jenis jadwal: Periodik

Parameter:

Parameter	Diperlukan	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`serviceNames`	Diperlukan	Nama layanan yang dievaluasi oleh kontrol	String	Tidak dapat disesuaikan	`ecr.api`
`vpcIds`	Opsional	Comma-separated daftar ID VPC Amazon untuk titik akhir VPC. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam `serviceName` parameter tidak memiliki salah satu titik akhir VPC ini.	StringList	Sesuaikan dengan satu atau lebih ID VPC	Tidak ada nilai default

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka untuk Amazon ECR API. Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk ECR API. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IP publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

Remediasi

Untuk mengonfigurasi titik akhir VPC, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan.AWS PrivateLink

[EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config aturan: vpc-endpoint-enabled

Jenis jadwal: Periodik

Parameter:

Parameter	Diperlukan	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`serviceNames`	Diperlukan	Nama layanan	String	Tidak dapat	`ecr.dkr`

Parameter	Diperlukan	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
		yang dievaluasi oleh kontrol		disesuaikan	
`vpcIds`	Opsional	Comma-separated daftar ID VPC Amazon untuk titik akhir VPC. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam `serviceName` parameter tidak memiliki salah satu titik akhir VPC ini.	StringList	Sesuaikan dengan satu atau lebih ID VPC	Tidak ada nilai default

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka untuk Docker Registry. Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Docker Registry. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IP publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

Remediasi

Untuk mengonfigurasi titik akhir VPC, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan.AWS PrivateLink

[EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config aturan: vpc-endpoint-enabled

Jenis jadwal: Periodik

Parameter:

Parameter	Diperlukan	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`serviceNames`	Diperlukan	Nama layanan	String	Tidak dapat	`ssm`

Parameter	Diperlukan	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
		yang dievaluasi oleh kontrol		disesuaikan	
`vpcIds`	Opsional	Comma-separated daftar ID VPC Amazon untuk titik akhir VPC. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam `serviceName` parameter tidak memiliki salah satu titik akhir VPC ini.	StringList	Sesuaikan dengan satu atau lebih ID VPC	Tidak ada nilai default

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka. AWS Systems Manager Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Systems Manager. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IP publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

Remediasi

Untuk mengonfigurasi titik akhir VPC, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan.AWS PrivateLink

[EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config aturan: vpc-endpoint-enabled

Jenis jadwal: Periodik

Parameter:

Parameter	Diperlukan	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`serviceNames`	Diperlukan	Nama layanan yang dievaluasi oleh kontrol	String	Tidak dapat disesuaikan	`ssm-contacts`
`vpcIds`	Opsional	Comma-separated daftar ID VPC Amazon untuk titik akhir VPC. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam `serviceName` parameter tidak memiliki salah satu titik akhir VPC ini.	StringList	Sesuaikan dengan satu atau lebih ID VPC	Tidak ada nilai default

Kontrol ini memeriksa apakah virtual private cloud (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka untuk Kontak Manajer Insiden. AWS Systems Manager Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IP publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

Remediasi

Untuk mengonfigurasi titik akhir VPC, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan.AWS PrivateLink

[EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Kategori: Lindungi > Manajemen akses yang aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config aturan: vpc-endpoint-enabled

Jenis jadwal: Periodik

Parameter:

Parameter	Diperlukan	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`serviceNames`	Diperlukan	Nama layanan yang dievaluasi oleh kontrol	String	Tidak dapat disesuaikan	`ssm-incidents`
`vpcIds`	Opsional	Comma-separated daftar ID VPC Amazon untuk titik akhir VPC. Jika disediakan, kontrol gagal jika layanan yang ditentukan dalam `serviceName` parameter tidak memiliki salah satu titik akhir VPC ini.	StringList	Sesuaikan dengan satu atau lebih ID VPC	Tidak ada nilai default

Kontrol ini memeriksa apakah cloud pribadi virtual (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka untuk Manajer Insiden. AWS Systems Manager Kontrol gagal jika VPC tidak memiliki titik akhir VPC antarmuka untuk Systems Manager Incident Manager. Kontrol ini mengevaluasi sumber daya dalam satu akun.

AWS PrivateLink memungkinkan pelanggan untuk mengakses layanan yang di-host dengan AWS cara yang sangat tersedia dan terukur, sambil menjaga semua lalu lintas jaringan dalam AWS jaringan. Pengguna layanan dapat secara pribadi mengakses layanan yang didukung oleh PrivateLink dari VPC atau lokal mereka, tanpa menggunakan IP publik, dan tanpa memerlukan lalu lintas untuk melintasi internet.

Remediasi

Untuk mengonfigurasi titik akhir VPC, lihat Mengakses titik akhir VPC antarmuka Layanan AWS menggunakan antarmuka di Panduan.AWS PrivateLink

[EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)

Persyaratan terkait: PCI DSS v4.0. 1/2.2.6

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::LaunchTemplate`

AWS Config aturan: ec2-launch-template-imdsv2-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah templat peluncuran Amazon EC2 dikonfigurasi dengan Layanan Metadata Instans Versi 2 (IMDSv2). Kontrol gagal jika `HttpTokens` diatur ke`optional`.

Menjalankan sumber daya pada versi perangkat lunak yang didukung memastikan kinerja, keamanan, dan akses optimal ke fitur-fitur terbaru. Pembaruan rutin melindungi terhadap kerentanan, yang membantu memastikan pengalaman pengguna yang stabil dan efisien.

Remediasi

Untuk mewajibkan IMDSv2 pada templat peluncuran EC2, lihat Mengonfigurasi opsi Layanan Metadata Instans di Panduan Pengguna Amazon EC2.

[EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging

Persyaratan terkait: CIS AWS Foundations Benchmark v3.0. 0/5.3, PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPNConnection`

AWS Config aturan: ec2-vpn-connection-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi AWS Site-to-Site VPN mengaktifkan Amazon CloudWatch Logs untuk kedua terowongan. Kontrol gagal jika koneksi Site-to-Site VPN tidak mengaktifkan CloudWatch Log untuk kedua terowongan.

AWS Site-to-Site Log VPN memberi Anda visibilitas yang lebih dalam ke penerapan Site-to-Site VPN Anda. Dengan fitur ini, Anda memiliki akses ke log koneksi Site-to-Site VPN yang memberikan rincian tentang pembentukan terowongan IP Security (IPsec), negosiasi Internet Key Exchange (IKE), dan pesan protokol deteksi rekan mati (DPD). Site-to-Site Log VPN dapat dipublikasikan ke CloudWatch Log. Fitur ini memberi pelanggan satu cara konsisten untuk mengakses dan menganalisis log terperinci untuk semua koneksi Site-to-Site VPN mereka.

Remediasi

Untuk mengaktifkan pencatatan terowongan pada koneksi VPN EC2, lihat log AWS Site-to-Site VPN di Panduan Pengguna AWS Site-to-Site VPN.

[EC2.172] Pengaturan Akses Publik Blok VPC EC2 harus memblokir lalu lintas gateway internet

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config aturan: `ec2-vpc-bpa-internet-gateway-blocked` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`vpcBpaInternetGatewayBlockMode`	Nilai string dari mode opsi VPC BPA.	Enum	`block-bidirectional` , `block-ingress`	Tidak ada nilai default

Kontrol ini memeriksa apakah pengaturan Amazon EC2 VPC Block Public Access (BPA) dikonfigurasi untuk memblokir lalu lintas gateway internet untuk semua VPC Amazon di. Akun AWS Kontrol gagal jika pengaturan VPC BPA tidak dikonfigurasi untuk memblokir lalu lintas gateway internet. Agar kontrol lolos, BPA VPC `InternetGatewayBlockMode` harus disetel ke atau. `block-bidirectional` `block-ingress` Jika parameter `vpcBpaInternetGatewayBlockMode` disediakan, kontrol hanya lewat jika nilai VPC BPA `InternetGatewayBlockMode` cocok dengan parameter.

Mengonfigurasi pengaturan BPA VPC untuk akun Anda di Wilayah AWS sebuah memungkinkan Anda memblokir sumber daya di VPC dan subnet yang Anda miliki di Wilayah itu agar tidak menjangkau atau dijangkau dari internet melalui gateway internet dan gateway internet khusus egres. Jika Anda memerlukan VPC dan subnet tertentu untuk dapat menjangkau atau dapat dijangkau dari internet, Anda dapat mengecualikannya dengan mengonfigurasi pengecualian VPC BPA. Untuk petunjuk cara membuat dan menghapus pengecualian, lihat Membuat dan menghapus pengecualian di Panduan Pengguna Amazon VPC.

Remediasi

Untuk mengaktifkan BPA dua arah di tingkat akun, lihat Mengaktifkan mode dua arah BPA untuk akun Anda di Panduan Pengguna Amazon VPC. Untuk mengaktifkan BPA khusus masuk, lihat Mengubah mode BPA VPC menjadi hanya masuk. Untuk mengaktifkan BPA VPC di tingkat Organisasi, lihat Mengaktifkan BPA VPC di tingkat Organisasi.

[EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::SpotFleet`

AWS Config aturan: ec2-spot-fleet-request-ct-encryption-at-rest

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah permintaan Amazon EC2 Spot Fleet yang menentukan parameter peluncuran dikonfigurasi untuk mengaktifkan enkripsi untuk semua volume Amazon Elastic Block Store (Amazon EBS) yang dilampirkan ke instans EC2. Kontrol gagal jika permintaan Armada Spot menentukan parameter peluncuran dan tidak mengaktifkan enkripsi untuk satu atau beberapa volume EBS yang ditentukan dalam permintaan.

Untuk lapisan keamanan tambahan, Anda harus mengaktifkan enkripsi untuk volume Amazon EBS. Operasi enkripsi kemudian terjadi pada server yang meng-host instans Amazon EC2, yang membantu memastikan keamanan data saat istirahat dan data dalam perjalanan antara instans dan penyimpanan EBS terlampir. Enkripsi Amazon EBS adalah solusi enkripsi langsung untuk sumber daya EBS yang terkait dengan instans EC2 Anda. Dengan enkripsi EBS, Anda tidak perlu membangun, memelihara, dan mengamankan infrastruktur manajemen kunci Anda sendiri. Enkripsi EBS digunakan AWS KMS keys saat membuat volume terenkripsi.

> **Catatan**
>
> Kontrol ini tidak menghasilkan temuan untuk permintaan Armada Spot Amazon EC2 yang menggunakan templat peluncuran. Ini juga tidak menghasilkan temuan untuk permintaan Spot Fleet yang tidak secara eksplisit menentukan nilai untuk parameter. `encrypted`

Remediasi

Tidak ada cara langsung untuk mengenkripsi volume Amazon EBS yang sudah ada dan tidak terenkripsi. Anda dapat mengenkripsi volume baru hanya ketika Anda membuatnya.

Namun, jika Anda mengaktifkan enkripsi secara default, Amazon EBS mengenkripsi volume baru dengan menggunakan kunci default Anda untuk enkripsi EBS. Jika Anda tidak mengaktifkan enkripsi secara default, Anda dapat mengaktifkan enkripsi saat membuat volume individual. Dalam kedua kasus tersebut, Anda dapat mengganti kunci default untuk enkripsi EBS dan memilih pelanggan yang dikelola. AWS KMS key Untuk informasi selengkapnya tentang enkripsi EBS, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.

Untuk informasi tentang membuat permintaan Armada Spot Amazon EC2, lihat Membuat Armada Spot di Panduan Pengguna Amazon Elastic Compute Cloud.

[EC2.174] Set opsi EC2 DHCP harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::DHCPOptions`

AWS Config aturan: ec2-dhcp-options-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah set opsi Amazon EC2 DHCP memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika set opsi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa

keberadaan kunci tag dan gagal jika set opsi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke set opsi Amazon EC2 DHCP, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.175] Templat peluncuran EC2 harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::LaunchTemplate`

AWS Config aturan: ec2-launch-template-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah template peluncuran Amazon EC2 memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika template peluncuran tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika templat peluncuran tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke templat peluncuran Amazon EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.176] Daftar awalan EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::PrefixList`

AWS Config aturan: ec2-prefix-list-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar awalan Amazon EC2 memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika daftar awalan tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika daftar awalan tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu

Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke daftar awalan Amazon EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.177] Sesi cermin lalu lintas EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TrafficMirrorSession`

AWS Config aturan: ec2-traffic-mirror-session-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluas	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	i. Kunci tag peka huruf besar dan kecil.		persyaratan AWS .	

Kontrol ini memeriksa apakah sesi cermin lalu lintas Amazon EC2 memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika sesi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sesi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke sesi cermin lalu lintas Amazon EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.178] Filter cermin lalu lintas EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TrafficMirrorFilter`

AWS Config aturan: ec2-traffic-mirror-filter-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah filter cermin lalu lintas Amazon EC2 memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika filter tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika filter tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke filter cermin lalu lintas Amazon EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.179] Target cermin lalu lintas EC2 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EC2::TrafficMirrorTarget`

AWS Config aturan: ec2-traffic-mirror-target-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratan AWS .	Tidak ada nilai default

Kontrol ini memeriksa apakah target mirror lalu lintas Amazon EC2 memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika target tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa

keberadaan kunci tag dan gagal jika target tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke target mirror lalu lintas Amazon EC2, lihat Menandai sumber daya Amazon EC2 Anda di Panduan Pengguna Amazon EC2.

[EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::NetworkInterface`

AWS Config aturan: ec2-enis-source-destination-check-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini source/destination memeriksa apakah pemeriksaan diaktifkan untuk elastic network interface (ENI) Amazon EC2 yang dikelola oleh pengguna. Kontrol gagal jika source/destination

pemeriksaan dinonaktifkan untuk ENI yang dikelola pengguna. Kontrol ini hanya memeriksa jenis ENI berikut:`aws_codestar_connections_managed`,,`branch`,`efa`, `interfacelambda`, dan`quicksight`.

Source/destination memeriksa instans Amazon EC2 dan ENI terlampir harus diaktifkan dan dikonfigurasi secara konsisten di seluruh instans EC2 Anda. Setiap ENI memiliki pengaturan sendiri untuk source/destination pemeriksaan. Jika source/destination pemeriksaan diaktifkan, Amazon EC2 memberlakukan validasi source/destination alamat, yang memastikan bahwa instance adalah sumber atau tujuan dari lalu lintas apa pun yang diterimanya. Ini memberikan lapisan tambahan keamanan jaringan dengan mencegah sumber daya menangani lalu lintas yang tidak diinginkan dan mencegah spoofing alamat IP.

> **Note**
>
> Jika Anda menggunakan instans EC2 sebagai instans NAT dan Anda menonaktifkan source/destination pemeriksaan ENI-nya, Anda dapat menggunakan gateway NAT sebagai gantinya.

Remediasi

Untuk informasi tentang mengaktifkan source/destination pemeriksaan untuk Amazon EC2 ENI, lihat Memodifikasi atribut antarmuka jaringan di Panduan Pengguna Amazon EC2.

[EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::LaunchTemplate`

AWS Config aturan: ec2-launch-templates-ebs-volume-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah template peluncuran Amazon EC2 memungkinkan enkripsi untuk semua volume EBS terlampir. Kontrol gagal jika parameter enkripsi disetel ke `False` volume EBS apa pun yang ditentukan oleh templat peluncuran EC2.

Enkripsi Amazon EBS adalah solusi enkripsi langsung untuk sumber daya EBS yang terkait dengan instans Amazon EC2. Dengan enkripsi EBS, Anda tidak perlu membangun, memelihara, dan mengamankan infrastruktur manajemen kunci Anda sendiri. Enkripsi EBS digunakan AWS KMS keys saat membuat volume dan snapshot terenkripsi. Operasi enkripsi terjadi pada server yang meng-host instans EC2, yang membantu memastikan keamanan data saat istirahat dan data dalam perjalanan antara instans EC2 dan penyimpanan EBS terlampir. Untuk informasi selengkapnya, lihat enkripsi Amazon EBS di Panduan Pengguna Amazon EBS.

Anda dapat mengaktifkan enkripsi EBS selama peluncuran manual instans EC2 individual. Namun, ada beberapa manfaat menggunakan templat peluncuran EC2 dan mengonfigurasi pengaturan enkripsi di templat tersebut. Anda dapat menerapkan enkripsi sebagai standar dan memastikan penggunaan pengaturan enkripsi yang konsisten. Anda juga dapat mengurangi risiko kesalahan dan kesenjangan keamanan yang mungkin terjadi dengan peluncuran instance secara manual.

> **Note**
>
> Ketika kontrol ini memeriksa template peluncuran EC2, itu hanya mengevaluasi pengaturan enkripsi EBS yang secara eksplisit ditentukan oleh template. Evaluasi tidak mencakup pengaturan enkripsi yang diwarisi dari pengaturan enkripsi EBS tingkat akun, pemetaan perangkat blok AMI, atau status enkripsi snapshot sumber.

Remediasi

Setelah Anda membuat template peluncuran Amazon EC2, Anda tidak dapat memodifikasinya. Namun, Anda dapat membuat versi baru dari template peluncuran dan mengubah pengaturan enkripsi di versi baru template tersebut. Anda juga dapat menentukan versi baru sebagai versi default dari template peluncuran. Kemudian, jika Anda meluncurkan instans EC2 dari template peluncuran dan tidak menentukan versi template, EC2 menggunakan pengaturan versi default saat meluncurkan instance. Untuk informasi selengkapnya, lihat Memodifikasi templat peluncuran di Panduan Pengguna Amazon EC2.

[EC2.182] Blokir pengaturan akses publik harus diaktifkan untuk snapshot Amazon EBS

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EC2::SnapshotBlockPublicAccess`

AWS Config aturan: ebs-snapshot-block-public-access

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses publik blok tingkat akun diaktifkan untuk mencegah berbagi snapshot Amazon EBS ke semua. Kontrol gagal jika memblokir akses publik tidak diaktifkan untuk memblokir berbagi snapshot Amazon EBS ke semua.

Untuk mencegah berbagi foto Amazon EBS secara publik, Anda dapat mengaktifkan blokir akses publik untuk snapshot. Setelah memblokir akses publik untuk snapshot diaktifkan di Wilayah, setiap upaya untuk membagikan snapshot secara publik di Wilayah tersebut akan diblokir secara otomatis. Ini membantu meningkatkan keamanan snapshot dan melindungi data snapshot dari akses yang tidak sah atau tidak diinginkan.

Remediasi

Untuk mengaktifkan blokir akses publik untuk snapshot, lihat Mengonfigurasi blokir akses publik untuk snapshot Amazon EBS di Panduan Pengguna Amazon EBS. Untuk Blokir akses publik, pilih Blokir semua akses publik.

[EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EC2::VPNConnection`

AWS Config aturan: ec2-vpn-connection-ike-version-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi AWS Site-to-Site VPN dikonfigurasi untuk menggunakan protokol IKEv2. Kontrol gagal jika koneksi Site-to-Site VPN memungkinkan protokol IKEv1 atau tidak secara eksplisit membatasi IKEv2 di semua terowongan VPN.

IKEv2 menyediakan algoritma kriptografi yang lebih kuat dan fitur keamanan yang lebih baik dibandingkan dengan protokol IKEv1 lama, termasuk perlindungan bawaan terhadap serangan denial-of-service dan mekanisme otentikasi yang ditingkatkan. IKEv1 telah mengetahui kerentanan

dan kelemahan dalam proses pertukaran utamanya yang dapat dimanfaatkan oleh penyerang untuk membahayakan keamanan terowongan VPN. Dengan menerapkan IKEv2-only koneksi, Anda mengurangi permukaan serangan dan memastikan komunikasi VPN menggunakan protokol enkripsi standar industri modern yang melindungi data saat transit dengan lebih baik.

Remediasi

Untuk memperbarui versi IKE untuk terowongan VPN pada koneksi VPN EC2, lihat Memodifikasi opsi terowongan AWS Site-to-Site AWS Site-to-Site VPN di Panduan Pengguna VPN.

Kontrol CSPM Security Hub untuk Auto Scaling

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon EC2 Auto Scaling.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB

Persyaratan terkait: PCI DSS v3.2. 1/2.2, NIST.800-53.r5 CA-7, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 SI-2

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Configaturan: **`autoscaling-group-elb-healthcheck-required`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup Amazon EC2 Auto Scaling yang terkait dengan penyeimbang beban menggunakan pemeriksaan kesehatan Elastic Load Balancing (ELB). Kontrol gagal jika grup Auto Scaling tidak menggunakan pemeriksaan kesehatan ELB.

Pemeriksaan kesehatan ELB membantu memastikan bahwa grup Auto Scaling dapat menentukan kesehatan instans berdasarkan tes tambahan yang disediakan oleh penyeimbang beban. Menggunakan pemeriksaan kesehatan Elastic Load Balancing juga membantu mendukung ketersediaan aplikasi yang menggunakan grup EC2 Auto Scaling.

Remediasi

Untuk menambahkan pemeriksaan kesehatan Elastic Load Balancing, lihat Menambahkan pemeriksaan kesehatan Menambahkan Elastic Load Balancing di Panduan Pengguna Amazon EC2 Auto Scaling.

[AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Configaturan: **`autoscaling-multiple-az`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub	
`minAvailabilityZones`	Jumlah minimum Availability Zone	Enum	`2, 3, 4, 5, 6`	`2`	

Kontrol ini memeriksa apakah grup Penskalaan Otomatis Amazon EC2 mencakup setidaknya jumlah Availability Zone (AZ) yang ditentukan. Kontrol gagal jika grup Auto Scaling tidak menjangkau setidaknya jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub CSPM menggunakan nilai default dua AZ.

Grup Auto Scaling yang tidak menjangkau beberapa AZ tidak dapat meluncurkan instance di AZ lain untuk mengkompensasi jika AZ tunggal yang dikonfigurasi menjadi tidak tersedia. Namun, grup Auto

Scaling dengan satu Availability Zone mungkin lebih disukai dalam beberapa kasus penggunaan, seperti pekerjaan batch atau ketika biaya transfer antar-AZ harus dijaga seminimal mungkin. Dalam kasus seperti itu, Anda dapat menonaktifkan kontrol ini atau menekan temuannya.

Remediasi

Untuk menambahkan AZ ke grup Auto Scaling yang ada, lihat Menambahkan dan menghapus Availability Zone di Panduan Pengguna Amazon EC2 Auto Scaling.

[AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)

Persyaratan terkait: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/2.2.6

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AutoScaling::LaunchConfiguration`

AWS Configaturan: **`autoscaling-launchconfig-requires-imdsv2`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah IMDSv2 diaktifkan pada semua instans yang diluncurkan oleh grup Amazon EC2 Auto Scaling. Kontrol gagal jika versi Instance Metadata Service (IMDS) tidak disertakan dalam konfigurasi peluncuran atau dikonfigurasi sebagai`token optional`, yang merupakan pengaturan yang memungkinkan IMDSv1 atau IMDSv2.

IMDS menyediakan data tentang instans yang dapat Anda gunakan untuk mengonfigurasi atau mengelola instance yang sedang berjalan.

IMDS versi 2 menambahkan perlindungan baru yang tidak tersedia di IMDSv1 untuk lebih melindungi instans EC2 Anda.

Remediasi

Grup Auto Scaling dikaitkan dengan satu konfigurasi peluncuran pada satu waktu. Anda tidak dapat mengubah konfigurasi peluncuran setelah Anda membuatnya. Untuk mengubah konfigurasi

peluncuran untuk grup Auto Scaling, gunakan konfigurasi peluncuran yang ada sebagai dasar untuk konfigurasi peluncuran baru dengan IMDSv2 diaktifkan. Untuk informasi selengkapnya, lihat Mengonfigurasi opsi metadata instans untuk instans baru di Panduan Pengguna Amazon EC2.

[AutoScaling.4] Konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki batas hop respons metadata yang lebih besar dari 1

> **Important**
>
> Security Hub CSPM menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Log perubahan untuk kontrol CSPM Security Hub.

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AutoScaling::LaunchConfiguration`

AWS Configaturan: **`autoscaling-launch-config-hop-limit`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa jumlah hop jaringan yang dapat ditempuh oleh token metadata. Kontrol gagal jika batas hop respons metadata lebih besar dari. 1

Layanan Metadata Instans (IMDS) menyediakan informasi metadata tentang instans Amazon EC2 dan berguna untuk konfigurasi aplikasi. Membatasi PUT respons HTTP untuk layanan metadata hanya untuk instans EC2 melindungi IMDS dari penggunaan yang tidak sah.

Bidang Time To Live (TTL) dalam paket IP dikurangi satu pada setiap hop. Pengurangan ini dapat digunakan untuk memastikan bahwa paket tidak bergerak di luar EC2. IMDSv2 melindungi instans EC2 yang mungkin salah dikonfigurasi sebagai router terbuka, firewall lapisan 3, VPN, terowongan, atau perangkat NAT, yang mencegah pengguna yang tidak sah mengambil metadata. Dengan ImDSv2, PUT respons yang berisi token rahasia tidak dapat berjalan di luar instance karena batas hop respons metadata default disetel ke. 1 Namun, jika nilai ini lebih besar dari1, token dapat meninggalkan instans EC2.

Remediasi

Untuk mengubah batas hop respons metadata untuk konfigurasi peluncuran yang ada, lihat Memodifikasi opsi metadata instans untuk instans yang ada di Panduan Pengguna Amazon EC2.

[Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AutoScaling::LaunchConfiguration`

AWS Configaturan: **`autoscaling-launch-config-public-ip-disabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konfigurasi peluncuran terkait grup Auto Scaling menetapkan alamat IP publik ke instans grup. Kontrol gagal jika konfigurasi peluncuran terkait menetapkan alamat IP publik.

Instans Amazon EC2 dalam konfigurasi peluncuran grup Auto Scaling tidak boleh memiliki alamat IP publik terkait, kecuali dalam kasus edge terbatas. Instans Amazon EC2 seharusnya hanya dapat diakses dari belakang penyeimbang beban alih-alih langsung terpapar ke internet.

Remediasi

Grup Auto Scaling dikaitkan dengan satu konfigurasi peluncuran pada satu waktu. Anda tidak dapat mengubah konfigurasi peluncuran setelah Anda membuatnya. Untuk mengubah konfigurasi peluncuran untuk grup Auto Scaling, gunakan konfigurasi peluncuran yang ada sebagai dasar untuk konfigurasi peluncuran baru. Lalu, perbarui grup Auto Scaling Anda untuk menggunakan konfigurasi peluncuran baru. Untuk petunjuk langkah demi langkah, lihat Mengubah konfigurasi peluncuran untuk

grup Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling. Saat membuat konfigurasi peluncuran baru, di bawah Konfigurasi tambahan, untuk detail lanjutan, jenis alamat IP, pilih Jangan tetapkan alamat IP publik ke instance apa pun.

Setelah Anda mengubah konfigurasi peluncuran, Auto Scaling meluncurkan instance baru dengan opsi konfigurasi baru. Instance yang ada tidak terpengaruh. Untuk memperbarui instans yang ada, kami sarankan Anda menyegarkan instans Anda, atau mengizinkan penskalaan otomatis untuk secara bertahap mengganti instans lama dengan instans yang lebih baru berdasarkan kebijakan penghentian Anda. Untuk informasi selengkapnya tentang memperbarui instans Auto Scaling, lihat Memperbarui instans Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.

[AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Configaturan: **`autoscaling-multiple-instance-types`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup Amazon EC2 Auto Scaling menggunakan beberapa jenis instans. Kontrol gagal jika grup Auto Scaling hanya memiliki satu jenis instance yang ditentukan.

Anda dapat meningkatkan ketersediaan dengan menerapkan aplikasi Anda di beberapa jenis instans yang berjalan di beberapa Availability Zone. Security Hub CSPM merekomendasikan penggunaan beberapa jenis instans sehingga grup Auto Scaling dapat meluncurkan jenis instans lain jika kapasitas instans tidak mencukupi di Availability Zone yang Anda pilih.

Remediasi

Untuk membuat grup Auto Scaling dengan beberapa jenis instans, lihat grup Auto Scaling dengan beberapa jenis instans dan opsi pembelian di Panduan Pengguna Amazon EC2 Auto Scaling.

[AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Configaturan: **`autoscaling-launch-template`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup Amazon EC2 Auto Scaling dibuat dari template peluncuran EC2. Kontrol ini gagal jika grup Penskalaan Otomatis Amazon EC2 tidak dibuat dengan templat peluncuran atau jika templat peluncuran tidak ditentukan dalam kebijakan instance campuran.

Grup EC2 Auto Scaling dapat dibuat dari templat peluncuran EC2 atau konfigurasi peluncuran. Namun, menggunakan template peluncuran untuk membuat grup Auto Scaling memastikan bahwa Anda memiliki akses ke fitur dan peningkatan terbaru.

Remediasi

Untuk membuat grup Auto Scaling dengan template peluncuran EC2, lihat Membuat grup Auto Scaling menggunakan template peluncuran di Panduan Pengguna Amazon EC2 Auto Scaling. Untuk informasi tentang cara mengganti konfigurasi peluncuran dengan templat peluncuran, lihat Mengganti konfigurasi peluncuran dengan templat peluncuran di Panduan Pengguna Amazon EC2.

[AutoScaling.10] Grup EC2 Auto Scaling harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AutoScaling::AutoScalingGroup`

AWS Configaturan: `tagged-autoscaling-autoscalinggroup` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah grup Amazon EC2 Auto Scaling memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup Auto Scaling tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup Auto Scaling tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup Auto Scaling, lihat Menandai grup dan instans Auto Scaling di Panduan Pengguna Amazon EC2 Auto Scaling.

Kontrol CSPM Hub Keamanan untuk Amazon ECR

Kontrol Security Hub CSPM ini mengevaluasi layanan dan sumber daya Amazon Elastic Container Registry (Amazon ECR).

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 RA-5, PCI DSS v4.0. 1/6.2.3, PCI DSS v4.0. 1/6.2.4

Kategori: Identifikasi > Kerentanan, patch, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECR::Repository`

AWS Config aturan: ecr-private-image-scanning-enabled

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori Amazon ECR pribadi memiliki pemindaian gambar yang dikonfigurasi. Kontrol gagal jika repositori ECR pribadi tidak dikonfigurasi untuk pemindaian saat push atau pemindaian berkelanjutan.

Pemindaian gambar ECR membantu mengidentifikasi kerentanan perangkat lunak dalam gambar kontainer Anda. Mengkonfigurasi pemindaian gambar pada repositori ECR menambahkan lapisan verifikasi untuk integritas dan keamanan gambar yang disimpan.

Remediasi

Untuk mengonfigurasi pemindaian gambar untuk repositori ECR, lihat Pemindaian gambar di Panduan Pengguna Amazon Elastic Container Registry.

[ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-8 (1)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECR::Repository`

AWS Config aturan: ecr-private-tag-immutability-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori ECR pribadi mengaktifkan kekekalan tag. Kontrol ini gagal jika repositori ECR pribadi menonaktifkan kekekalan tag. Aturan ini lolos jika kekekalan tag diaktifkan dan memiliki nilai. `IMMUTABLE`

Amazon ECR Tag Immutability memungkinkan pelanggan mengandalkan tag deskriptif gambar sebagai mekanisme yang andal untuk melacak dan mengidentifikasi gambar secara unik. Tag yang tidak dapat diubah bersifat statis, yang berarti setiap tag mengacu pada gambar yang unik. Ini meningkatkan keandalan dan skalabilitas karena penggunaan tag statis akan selalu menghasilkan gambar yang sama yang digunakan. Saat dikonfigurasi, kekekalan tag mencegah tag diganti, yang mengurangi permukaan serangan.

Remediasi

Untuk membuat repositori dengan tag yang tidak dapat diubah dikonfigurasi atau memperbarui pengaturan mutabilitas tag gambar untuk repositori yang ada, lihat Mutabilitas tag gambar di Panduan Pengguna Amazon Elastic Container Registry.

[ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECR::Repository`

AWS Config aturan: ecr-private-lifecycle-policy-configured

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah repositori Amazon ECR memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi. Kontrol ini gagal jika repositori ECR tidak memiliki kebijakan siklus hidup yang dikonfigurasi.

Kebijakan siklus hidup Amazon ECR memungkinkan Anda untuk menentukan manajemen siklus hidup citra dalam repositori. Dengan mengonfigurasi kebijakan siklus hidup, Anda dapat mengotomatiskan pembersihan gambar yang tidak digunakan dan kedaluwarsa gambar berdasarkan usia atau jumlah. Mengotomatiskan tugas-tugas ini dapat membantu Anda menghindari penggunaan gambar usang secara tidak sengaja di repositori Anda.

Remediasi

Untuk mengonfigurasi kebijakan siklus hidup, lihat Membuat pratinjau kebijakan siklus hidup di Panduan Pengguna Amazon Elastic Container Registry.

[ECR.4] Repositori publik ECR harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECR::PublicRepository`

AWS Config aturan: `tagged-ecr-publicrepository` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah repositori publik Amazon ECR memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika repositori publik tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika repositori publik tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke repositori publik ECR, lihat Men andai repositori publik Amazon ECR di Panduan Pengguna Amazon Elastic Container Registry.

[ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys

Persyaratan terkait: NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28,, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 SI-7 (6), NIST.800-53.r5 AU-9

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECR::Repository`

AWS Config aturan: ecr-repository-cmk-encryption-enabled

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`kmsKeyArns`	Daftar Nama Sumber Daya Amazon (ARN) AWS KMS keys untuk disertakan dalam evaluasi. Kontrol menghasilkan tem `FAILED` uan jika repositori ECR tidak dienkripsi dengan kunci KMS dalam daftar.	StringList (maksimal 10 item)	1—10 ARN dari kunci KMS yang ada. Misalnya: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-`	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
			`123456789 0ab`	

Kontrol ini memeriksa apakah repositori Amazon ECR dienkripsi saat diam dengan pengelolaan pelanggan AWS KMS key. Kontrol gagal jika repositori ECR tidak dienkripsi dengan kunci KMS yang dikelola pelanggan. Anda dapat secara opsional menentukan daftar kunci KMS untuk kontrol untuk disertakan dalam evaluasi.

Secara default, Amazon ECR mengenkripsi data repositori dengan kunci terkelola Amazon S3 (SSE-S3), menggunakan AES-256 algoritma. Untuk kontrol tambahan, Anda dapat mengonfigurasi Amazon ECR untuk mengenkripsi data dengan AWS KMS key (SSE-KMS atau DSSE-KMS) sebagai gantinya. Kunci KMS dapat berupa: Kunci yang dikelola AWS yang dibuat dan dikelola Amazon ECR untuk Anda dan memiliki alias`aws/ecr`, atau kunci yang dikelola pelanggan yang Anda buat dan kelola di Anda Akun AWS. Dengan kunci KMS yang dikelola pelanggan, Anda memiliki kontrol penuh atas kunci tersebut. Ini termasuk mendefinisikan dan memelihara kebijakan kunci, mengelola hibah, memutar materi kriptografi, menetapkan tag, membuat alias, dan mengaktifkan dan menonaktifkan kunci.

> **Note**
>
> AWS KMS mendukung akses lintas akun ke kunci KMS. Jika repositori ECR dienkripsi dengan kunci KMS yang dimiliki oleh akun lain, kontrol ini tidak melakukan pemeriksaan lintas akun saat mengevaluasi repositori. Kontrol tidak menilai apakah Amazon ECR dapat mengakses dan menggunakan kunci saat melakukan operasi kriptografi untuk repositori.

Remediasi

Anda tidak dapat mengubah pengaturan enkripsi untuk repositori ECR yang ada. Namun, Anda dapat menentukan pengaturan enkripsi yang berbeda untuk repositori ECR yang kemudian Anda buat. Amazon ECR mendukung penggunaan pengaturan enkripsi yang berbeda untuk repositori individu.

Untuk informasi selengkapnya tentang opsi enkripsi untuk repositori ECR, lihat Enkripsi saat diam di Panduan Pengguna Amazon ECR. Untuk informasi selengkapnya tentang pengelolaan pelanggan AWS KMS keys, lihat AWS KMS keys di Panduan AWS Key Management Service Pengembang.

Kontrol CSPM Security Hub untuk Amazon ECS

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon Elastic Container Service (Amazon ECS). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::Service`

AWS Configaturan: `ecs-service-assign-public-ip-disabled` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah layanan Amazon ECS dikonfigurasi untuk secara otomatis menetapkan alamat IP publik. Kontrol ini gagal jika `AssignPublicIP` ada`ENABLED`. Kontrol ini lolos jika `AssignPublicIP` ada`DISABLED`.

Alamat IP publik adalah alamat IP yang dapat dijangkau dari internet. Jika Anda meluncurkan instans Amazon ECS Anda dengan alamat IP publik, maka instans Amazon ECS Anda dapat dijangkau dari internet. Layanan Amazon ECS tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke server aplikasi kontainer Anda.

Remediasi

Pertama, Anda harus membuat definisi tugas untuk cluster Anda yang menggunakan mode `awsvpc` jaringan dan menentukan FARGATE untuk. `requiresCompatibilities` Kemudian, untuk konfigurasi Compute, pilih Launch type dan FARGATE. Terakhir, untuk bidang Jaringan, matikan IP Publik untuk menonaktifkan penugasan IP publik otomatis untuk layanan Anda.

[ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-task-definition-pid-mode-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi tugas Amazon ECS dikonfigurasi untuk berbagi namespace proses host dengan kontainernya. Kontrol gagal jika definisi tugas membagikan namespace proses host dengan wadah yang berjalan di atasnya. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Namespace ID proses (PID) menyediakan pemisahan antar proses. Ini mencegah proses sistem agar tidak terlihat, dan memungkinkan PID untuk digunakan kembali, termasuk PID 1. Jika namespace PID host dibagikan dengan kontainer, itu akan memungkinkan kontainer untuk melihat semua proses pada sistem host. Ini mengurangi manfaat isolasi tingkat proses antara host dan wadah. Keadaan ini dapat menyebabkan akses tidak sah ke proses pada host itu sendiri, termasuk kemampuan untuk memanipulasi dan menghentikannya. Pelanggan tidak boleh membagikan namespace proses host dengan wadah yang berjalan di atasnya.

Remediasi

Untuk mengonfigurasi definisi tugas, lihat Parameter definisi tugas di Panduan Pengembang Layanan Amazon Elastic Container. `pidMode`

[ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-containers-nonprivileged

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah `privileged` parameter dalam definisi penampung Definisi Tugas Amazon ECS disetel ke`true`. Kontrol gagal jika parameter ini sama dengan`true`. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Kami menyarankan Anda menghapus hak istimewa yang ditinggikan dari definisi tugas ECS Anda. Ketika parameter privilege adalah`true`, penampung diberikan hak istimewa yang ditinggikan pada instance wadah host (mirip dengan pengguna root).

Remediasi

Untuk mengonfigurasi `privileged` parameter pada definisi tugas, lihat Parameter definisi kontainer lanjutan di Panduan Pengembang Layanan Kontainer Elastis Amazon.

[ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-containers-readonly-access

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi tugas ECS mengonfigurasi kontainer agar dibatasi pada akses hanya-baca ke sistem file root yang dipasang. Kontrol gagal jika `readonlyRootFilesystem` parameter dalam definisi wadah definisi tugas ECS disetel ke`false`, atau parameter tidak ada dalam definisi wadah dalam definisi tugas. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

Jika `readonlyRootFilesystem` parameter disetel ke `true` dalam definisi tugas Amazon ECS, wadah ECS diberikan akses hanya-baca ke sistem file root-nya. Ini mengurangi vektor serangan keamanan karena sistem file root instance container tidak dapat dirusak atau ditulis tanpa mount volume eksplisit yang memiliki izin baca-tulis untuk folder dan direktori sistem file. Mengaktifkan opsi ini juga mematuhi prinsip hak istimewa paling sedikit.

> **Note**
>
> `readonlyRootFilesystem`Parameter tidak didukung untuk wadah Windows. Definisi tugas dengan `runtimePlatform` dikonfigurasi untuk menentukan keluarga `WINDOWS_SERVER` OS ditandai sebagai `NOT_APPLICABLE` dan tidak akan menghasilkan temuan untuk kontrol ini.

Remediasi

Untuk memberikan akses read-only container Amazon ECS ke sistem file root, tambahkan `readonlyRootFilesystem` parameter ke definisi tugas untuk container, dan tetapkan nilai untuk parameter tersebut. `true` Untuk informasi tentang parameter definisi tugas dan cara menambahkannya ke definisi tugas, lihat definisi tugas Amazon ECS dan Memperbarui definisi tugas di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/8.6.2

Kategori: Lindungi > Pengembangan aman > Kredensyal tidak dikodekan dengan keras

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-no-environment-secrets

Jenis jadwal: Perubahan dipicu

Parameter:`secretKeys`:`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, `ECS_ENGINE_AUTH_DATA` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah nilai kunci dari setiap variabel dalam `environment` parameter definisi kontainer termasuk`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, atau`ECS_ENGINE_AUTH_DATA`. Kontrol ini gagal jika variabel lingkungan tunggal dalam definisi kontainer sama`AWS_ACCESS_KEY_ID`,`AWS_SECRET_ACCESS_KEY`, atau`ECS_ENGINE_AUTH_DATA`. Kontrol ini tidak mencakup variabel lingkungan yang diteruskan dari lokasi lain seperti Amazon S3. Kontrol ini hanya mengevaluasi revisi aktif terbaru dari definisi tugas Amazon ECS.

AWS Systems ManagerParameter Store dapat membantu Anda meningkatkan postur keamanan organisasi Anda. Sebaiknya gunakan Parameter Store untuk menyimpan rahasia dan kredensyal alih-alih langsung meneruskannya ke instance kontainer Anda atau mengkodekannya dengan keras ke dalam kode Anda.

Remediasi

Untuk membuat parameter menggunakan SSM, lihat Membuat parameter Systems Manager di Panduan AWS Systems Manager Pengguna. Untuk informasi selengkapnya tentang membuat definisi tugas yang menentukan rahasia, lihat Menentukan data sensitif menggunakan Secrets Manager di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging

Persyaratan terkait: NIST.800-53.r5 AC-4 (26) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-task-definition-log-configuration

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi tugas Amazon ECS aktif terbaru memiliki konfigurasi logging yang ditentukan. Kontrol gagal jika definisi tugas tidak memiliki `logConfiguration` properti yang ditentukan atau jika nilai untuk `logDriver` adalah nol dalam setidaknya satu definisi kontainer.

Logging membantu Anda menjaga keandalan, ketersediaan, dan kinerja Amazon ECS. Mengumpulkan data dari definisi tugas memberikan visibilitas, yang dapat membantu Anda men-debug proses dan menemukan akar penyebab kesalahan. Jika Anda menggunakan solusi logging yang tidak harus didefinisikan dalam definisi tugas ECS (seperti solusi logging pihak ketiga), Anda dapat menonaktifkan kontrol ini setelah memastikan bahwa log Anda ditangkap dan dikirim dengan benar.

Remediasi

Untuk menentukan konfigurasi log untuk definisi tugas Amazon ECS Anda, lihat Menentukan konfigurasi log dalam definisi tugas Anda di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru

Persyaratan terkait: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::Service`

AWS Configaturan: ecs-fargate-latest-platform-version

Jenis jadwal: Perubahan dipicu

Parameter:

- `latestLinuxVersion: 1.4.0`(tidak dapat disesuaikan)
- `latestWindowsVersion: 1.0.0`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah layanan Amazon ECS Fargate menjalankan versi platform Fargate terbaru. Kontrol ini gagal jika versi platform bukan yang terbaru.

AWS FargateVersi platform mengacu pada lingkungan runtime tertentu untuk infrastruktur tugas Fargate, yang merupakan kombinasi dari versi runtime kernel dan container. Versi platform baru

dirilis saat lingkungan runtime berkembang. Misalnya, versi baru dapat dirilis untuk pembaruan kernel atau sistem operasi, fitur baru, perbaikan bug, atau pembaruan keamanan. Pembaruan dan tambalan keamanan diterapkan secara otomatis untuk tugas Fargate Anda. Jika ditemukan masalah keamanan yang memengaruhi versi platform, AWS tambal versi platform.

Remediasi

Untuk memperbarui layanan yang ada, termasuk versi platformnya, lihat Memperbarui layanan di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer

Persyaratan terkait: NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::Cluster`

AWS Configaturan: ecs-container-insights-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster ECS menggunakan Wawasan Kontainer. Kontrol ini gagal jika Wawasan Kontainer tidak disiapkan untuk klaster.

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja klaster Amazon ECS. Gunakan CloudWatch Wawasan Kontainer untuk mengumpulkan, menggabungkan, dan meringkas metrik dan log dari aplikasi dan layanan mikro dalam kontainer Anda. CloudWatch Secara otomatis mengumpulkan metrik untuk banyak sumber daya, seperti CPU, memori, disk, dan jaringan. Wawasan Kontainer juga akan menyediakan informasi diagnostik, seperti kegagalan mengulang kembali kontainer, untuk membantu Anda melakukan isolasi atas masalah dan mengatasi masalah itu dengan cepat. Anda juga dapat menyetel CloudWatch alarm pada metrik yang dikumpulkan Container Insights.

Remediasi

Untuk menggunakan Wawasan Penampung, lihat Memperbarui layanan di Panduan CloudWatch Pengguna Amazon.

[ECS.13] Layanan ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECS::Service`

AWS Configaturan: `tagged-ecs-service` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah layanan Amazon ECS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika layanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika layanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke layanan ECS, lihat Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.14] Cluster ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECS::Cluster`

AWS Configaturan: `tagged-ecs-cluster` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratanAWS.	

Kontrol ini memeriksa apakah klaster Amazon ECS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke cluster ECS, lihat Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.15] Definisi tugas ECS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: `tagged-ecs-taskdefinition` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah definisi tugas Amazon ECS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika definisi tugas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika definisi tugas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke definisi tugas ECS, lihat Menandai resource Amazon ECS Anda di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik

Persyaratan terkait: PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ECS::TaskSet`

AWS Configaturan: `ecs-taskset-assign-public-ip-disabled` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah set tugas Amazon ECS dikonfigurasi untuk secara otomatis menetapkan alamat IP publik. Kontrol gagal jika `AssignPublicIP` disetel ke`ENABLED`.

Alamat IP publik dapat dijangkau dari internet. Jika Anda mengonfigurasi set tugas Anda dengan alamat IP publik, sumber daya yang terkait dengan kumpulan tugas dapat dijangkau dari internet.

Kumpulan tugas ECS tidak boleh diakses publik, karena ini memungkinkan akses yang tidak diinginkan ke server aplikasi kontainer Anda.

Remediasi

Untuk memperbarui set tugas ECS agar tidak menggunakan alamat IP publik, lihat Memperbarui definisi tugas Amazon ECS menggunakan konsol di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-task-definition-network-mode-not-host

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah revisi aktif terbaru dari definisi tugas Amazon ECS menggunakan mode `host` jaringan. Kontrol gagal jika revisi aktif terbaru dari definisi tugas ECS menggunakan mode `host` jaringan.

Saat menggunakan mode `host` jaringan, jaringan wadah Amazon ECS terikat langsung ke host yang mendasari yang menjalankan penampung. Akibatnya, mode ini memungkinkan kontainer untuk terhubung ke layanan jaringan loopback pribadi pada host dan untuk meniru host. Kelemahan signifikan lainnya adalah tidak ada cara untuk memetakan ulang port kontainer saat menggunakan mode `host` jaringan, dan Anda tidak dapat menjalankan lebih dari satu instance tugas di setiap host.

Remediasi

Untuk informasi tentang mode jaringan dan opsi untuk tugas Amazon ECS yang dihosting di instans Amazon EC2, lihat opsi jaringan tugas Amazon ECS untuk jenis peluncuran EC2 di Panduan Pengembang Layanan Kontainer Elastis Amazon. Untuk informasi tentang membuat revisi baru

definisi tugas dan menentukan mode jaringan yang berbeda, lihat Memperbarui definisi tugas Amazon ECS dalam panduan tersebut.

Jika definisi tugas Amazon ECS dibuat olehAWS Batch, lihat Mode jaringan untuk AWS Batch pekerjaan untuk mempelajari tentang mode jaringan dan penggunaan umum untuk jenis AWS Batch pekerjaan dan untuk memilih opsi yang aman.

[ECS.18] Definisi Tugas ECS harus menggunakan enkripsi dalam transit untuk volume EFS

Kategori: Lindungi > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-task-definition-efs-encryption-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah revisi aktif terbaru dari definisi tugas Amazon ECS menggunakan enkripsi dalam transit untuk volume EFS. Kontrol gagal jika revisi aktif terbaru dari definisi tugas ECS memiliki enkripsi dalam transit dinonaktifkan untuk volume EFS.

Volume Amazon EFS menyediakan penyimpanan file bersama yang sederhana, dapat diskalakan, dan persisten untuk digunakan dengan tugas Amazon ECS Anda. Amazon EFS mendukung enkripsi data dalam perjalanan dengan Transport Layer Security (TLS). Saat enkripsi data dalam perjalanan dinyatakan sebagai opsi pemasangan untuk sistem file EFS Anda, Amazon EFS membuat koneksi TLS yang aman dengan sistem file EFS Anda saat memasang sistem file Anda.

Remediasi

Untuk informasi tentang mengaktifkan enkripsi dalam perjalanan untuk Definisi Tugas Amazon ECS dengan volume EFS, lihat Langkah 5: Membuat definisi tugas di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.19] Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi yang dikelola

Kategori: Lindungi > Perlindungan Data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::CapacityProvider`

AWS Configaturan: ecs-capacity-provider-termination-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penyedia kapasitas Amazon ECS telah mengelola perlindungan penghentian yang diaktifkan. Kontrol gagal jika perlindungan terminasi terkelola tidak diaktifkan pada penyedia kapasitas ECS.

Penyedia kapasitas Amazon ECS mengelola penskalaan infrastruktur untuk tugas di cluster Anda. Saat menggunakan instans EC2 untuk kapasitas Anda, Anda menggunakan grup Auto Scaling untuk mengelola instans EC2. Perlindungan terminasi terkelola memungkinkan penskalaan otomatis cluster untuk mengontrol instance mana yang dihentikan. Saat Anda menggunakan perlindungan penghentian terkelola, Amazon ECS hanya menghentikan instans EC2 yang tidak menjalankan tugas Amazon ECS.

> **Note**
>
> Saat menggunakan perlindungan terminasi terkelola, penskalaan terkelola juga harus digunakan jika tidak, perlindungan terminasi terkelola tidak berfungsi.

Remediasi

Untuk mengaktifkan perlindungan penghentian terkelola bagi penyedia kapasitas Amazon ECS, lihat Memperbarui perlindungan penghentian terkelola untuk penyedia kapasitas Amazon ECS di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.20] Definisi Tugas ECS harus mengkonfigurasi pengguna non-root dalam definisi wadah Linux

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-task-definition-linux-user-non-root

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah revisi aktif terbaru dari definisi tugas Amazon ECS mengonfigurasi wadah Linux untuk dijalankan sebagai pengguna non-root. Kontrol gagal jika pengguna root default dikonfigurasi atau konfigurasi pengguna tidak ada untuk wadah apa pun.

Ketika wadah Linux berjalan dengan hak akses root, mereka menimbulkan beberapa risiko keamanan yang signifikan. Pengguna root memiliki akses tidak terbatas di dalam wadah. Akses yang meningkat ini meningkatkan risiko serangan pelarian kontainer, di mana penyerang berpotensi keluar dari isolasi kontainer dan mengakses sistem host yang mendasarinya. Jika kontainer yang berjalan sebagai root dikompromikan, penyerang dapat mengeksploitasi ini untuk mengakses atau memodifikasi sumber daya sistem host, yang memengaruhi wadah lain atau host itu sendiri. Selain itu, akses root dapat mengaktifkan serangan eskalasi hak istimewa, memungkinkan penyerang untuk mendapatkan izin tambahan di luar cakupan wadah yang dimaksudkan. Parameter pengguna dalam definisi tugas ECS dapat menentukan pengguna dalam beberapa format, termasuk nama pengguna, ID pengguna, nama pengguna dengan grup, atau UID dengan ID grup. Penting untuk mengetahui berbagai format ini saat mengonfigurasi definisi tugas untuk memastikan tidak ada akses root yang diberikan secara tidak sengaja. Mengikuti prinsip hak istimewa terkecil, kontainer harus berjalan dengan izin minimum yang diperlukan menggunakan pengguna non-root. Pendekatan ini secara signifikan mengurangi potensi permukaan serangan dan mengurangi dampak dari potensi pelanggaran keamanan.

> **Note**
>
> Kontrol ini hanya mengevaluasi definisi wadah dalam definisi tugas jika `operatingSystemFamily` dikonfigurasi sebagai `LINUX` atau tidak `operatingSystemFamily` dikonfigurasi dalam definisi tugas. Kontrol akan menghasilkan `FAILED` temuan untuk definisi tugas yang dievaluasi jika definisi wadah apa pun dalam definisi tugas `user` belum dikonfigurasi atau `user` dikonfigurasi sebagai pengguna root default. Pengguna root default untuk `LINUX` kontainer adalah `"root"` dan`"0"`.

Remediasi

Untuk informasi tentang membuat revisi baru Definisi Tugas Amazon ECS dan memperbarui `user` parameter dalam definisi container, lihat Memperbarui definisi tugas Amazon ECS di Panduan Pengembang Layanan Amazon Elastic Container.

[ECS.21] Definisi Tugas ECS harus mengkonfigurasi pengguna non-administrator dalam definisi wadah Windows

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ECS::TaskDefinition`

AWS Configaturan: ecs-task-definition-windows-user-non-admin

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah revisi aktif terbaru dari definisi tugas Amazon ECS mengonfigurasi wadah Windows untuk dijalankan sebagai pengguna yang bukan administrator default. Kontrol gagal jika administrator default dikonfigurasi sebagai konfigurasi pengguna atau pengguna tidak ada untuk wadah apa pun.

Ketika wadah Windows berjalan dengan hak administrator, mereka menimbulkan beberapa risiko keamanan yang signifikan. Administrator memiliki akses tak terbatas di dalam wadah. Akses yang meningkat ini meningkatkan risiko serangan pelarian kontainer, di mana penyerang berpotensi keluar dari isolasi kontainer dan mengakses sistem host yang mendasarinya.

> **Note**
>
> Kontrol ini hanya mengevaluasi definisi wadah dalam definisi tugas jika `operatingSystemFamily` dikonfigurasi sebagai `WINDOWS_SERVER` atau tidak `operatingSystemFamily` dikonfigurasi dalam definisi tugas. Kontrol akan menghasilkan `FAILED` temuan untuk definisi tugas yang dievaluasi jika definisi kontainer apa pun dalam definisi tugas `user` belum dikonfigurasi atau `user` dikonfigurasi sebagai administrator default untuk `WINDOWS_SERVER` wadah yang`"containeradministrator"`.

Remediasi

Untuk informasi tentang membuat revisi baru Definisi Tugas Amazon ECS dan memperbarui `user` parameter dalam definisi container, lihat Memperbarui definisi tugas Amazon ECS di Panduan Pengembang Layanan Amazon Elastic Container.

Kontrol CSPM Hub Keamanan untuk Amazon EFS

Kontrol Security Hub CSPM ini mengevaluasi layanan dan sumber daya Amazon Elastic File System (Amazon EFS). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.3.1, Benchmark Yay AWS asan CIS v3.0. 0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: efs-encrypted-check

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon Elastic File System dikonfigurasi untuk mengenkripsi data file menggunakan AWS KMS. Pemeriksaan gagal dalam kasus-kasus berikut.

- `Encrypted`diatur ke `false` dalam tang `DescribeFileSystems` gapan.
- K `KmsKeyId` unci dalam `DescribeFileSystems` respons tidak cocok dengan `KmsKeyId` parameter untuk `efs-encrypted-check`.

Perhatikan bahwa kontrol ini tidak menggunakan `KmsKeyId` parameter untuk `efs-encrypted-check`. Itu hanya memeriksa nilai`Encrypted`.

Untuk lapisan keamanan tambahan untuk data sensitif Anda di Amazon EFS, Anda harus membuat sistem file terenkripsi. Amazon EFS mendukung enkripsi untuk sistem file dalam keadaan diam. Anda dapat mengaktifkan enkripsi data saat diam saat membuat sistem file Amazon EFS. Untuk mempelajari lebih lanjut tentang enkripsi Amazon EFS, lihat Enkripsi data di Amazon EFS di Panduan Pengguna Sistem File Amazon Elastic.

Remediasi

Untuk detail tentang cara mengenkripsi sistem file Amazon EFS baru, lihat Mengen kripsi data saat diam di Panduan Pengguna Sistem File Amazon Elastic.

[EFS.2] Volume Amazon EFS harus dalam rencana cadangan

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Cadangan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: efs-in-backup-plan

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon Elastic File System (Amazon EFS) ditambahkan ke rencana cadangan di AWS Backup. Kontrol gagal jika sistem file Amazon EFS tidak disertakan dalam rencana cadangan.

Memasukkan sistem file EFS dalam rencana cadangan membantu Anda melindungi data Anda dari penghapusan dan kehilangan data.

Remediasi

Untuk mengaktifkan pencadangan otomatis untuk sistem file Amazon EFS yang ada, lihat Memulai 4: Membuat cadangan otomatis Amazon EFS di Panduan Peng AWS Backup embang.

[EFS.3] Titik akses EFS harus menerapkan direktori root

Persyaratan terkait: NIST.800-53.r5 AC-6 (10)

Kategori: Lindungi > Manajemen akses aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::AccessPoint`

AWS Config aturan: efs-access-point-enforce-root-directory

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon EFS dikonfigurasi untuk menerapkan direktori root. Kontrol gagal jika nilai `Path` diatur ke `/` (direktori root default dari sistem file).

Saat Anda menerapkan direktori root, klien NFS menggunakan titik akses menggunakan direktori root yang dikonfigurasi pada titik akses alih-alih direktori root sistem file. Menegakkan direktori root untuk titik akses membantu membatasi akses data dengan memastikan bahwa pengguna titik akses hanya dapat menjangkau file dari subdirektori yang ditentukan.

Remediasi

Untuk petunjuk tentang cara menerapkan direktori root untuk titik akses Amazon EFS, lihat Men egakkan direktori root dengan titik akses di Panduan Pengguna Sistem File Amazon Elastic.

[EFS.4] Titik akses EFS harus menegakkan identitas pengguna

Persyaratan terkait: NIST.800-53.r5 AC-6 (2), PCI DSS v4.0. 1/7.3.1

Kategori: Lindungi > Manajemen akses aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::AccessPoint`

AWS Config aturan: efs-access-point-enforce-user-identity

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon EFS dikonfigurasi untuk menegakkan identitas pengguna. Kontrol ini gagal jika identitas pengguna POSIX tidak ditentukan saat membuat titik akses EFS.

Titik akses Amazon EFS adalah titik masuk khusus aplikasi ke dalam sistem file EFS yang memudahkan pengelolaan akses aplikasi ke kumpulan data bersama. Titik akses dapat menerapkan

identitas pengguna, termasuk grup POSIX pengguna, pada semua permintaan sistem file yang dibuat melalui titik akses. Titik akses juga dapat menerapkan direktori asal yang berbeda untuk sistem file sehingga klien hanya dapat mengakses data dalam direktori tertentu atau subdirektorinya.

Remediasi

Untuk menerapkan identitas pengguna untuk titik akses Amazon EFS, lihat Men egakkan identitas pengguna menggunakan titik akses di Panduan Pengguna Sistem File Amazon Elastic.

[EFS.5] Titik akses EFS harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EFS::AccessPoint`

AWS Config aturan: `tagged-efs-accesspoint` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah titik akses Amazon EFS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika titik akses tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika titik akses tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke titik akses EFS, lihat Men andai sumber daya Amazon EFS di Panduan Pengguna Sistem File Amazon Elastic.

[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan

Persyaratan terkait: NIST.800-53.r5 SC-7, NIST.800-171.r2 3.1.20, PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Keamanan jaringan > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: efs-mount-target-public-accessible

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah target pemasangan Amazon EFS dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan. Kontrol gagal jika target mount dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan.

Subnet memiliki atribut yang menentukan apakah antarmuka jaringan yang dibuat di subnet secara otomatis menerima alamat IP publik. Untuk IPv4, `MapPublicIpOnLaunch` atribut disetel ke untuk subnet default dan `TRUE` `FALSE` untuk subnet nondefault (dengan pengecualian untuk subnet nondefault yang dibuat melalui wizard instance peluncuran EC2, yang disetel ke). `TRUE` Untuk IPv6, `AssignIpv6AddressOnCreation` atribut diatur ke `FALSE` untuk semua subnet secara default.

Meskipun target pemasangan Amazon EFS tidak dapat ditetapkan alamat IPv4 publik, menempatkannya di subnet yang dikonfigurasi untuk menetapkan alamat IP publik saat diluncurkan menunjukkan bahwa instans yang ditempatkan bersama yang diluncurkan di subnet tersebut yang mungkin memasang sistem file EFS dapat secara otomatis menerima alamat IP publik, yang dapat berisiko data sistem file dapat diakses dari host yang dialamatkan publik.

Pasang target di subnet dengan alamat IPv6 publik yang menetapkan otomatis diaktifkan dapat menerima alamat IPv6 yang dapat dirutekan secara global.

> **Note**
>
> Pada 3 Agustus 2026, Security Hub CSPM menghapus kontrol ini dari standar AWS Foundational Security Best Practices (FSBP). Kontrol ini akan tersedia dalam standar NIST SP 800-53 Rev. 5, standar NIST SP 800-171 Revisi 2, dan standar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html

Remediasi

Untuk mengaitkan target pemasangan yang ada dengan subnet yang berbeda, Anda harus membuat target pemasangan baru di subnet yang tidak menetapkan alamat IP publik saat peluncuran dan kemudian menghapus target pemasangan lama. Untuk informasi tentang mengelola target pemasangan, lihat Membuat dan mengelola target pemasangan dan grup keamanan di Panduan Pengguna Sistem File Amazon Elastic.

[EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis

Kategori: Puli hkan > Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: efs-automatic-backups-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon EFS mengaktifkan pencadangan otomatis. Kontrol ini gagal jika sistem file EFS tidak mengaktifkan pencadangan otomatis.

Cadangan data adalah salinan sistem, konfigurasi, atau data aplikasi Anda yang disimpan secara terpisah dari aslinya. Mengaktifkan pencadangan reguler membantu Anda melindungi data berharga dari kejadian tak terduga seperti kegagalan sistem, serangan dunia maya, atau penghapusan yang tidak disengaja. Memiliki strategi pencadangan yang kuat juga memfasilitasi pemulihan yang lebih cepat, kelangsungan bisnis, dan ketenangan pikiran dalam menghadapi potensi kehilangan data.

Remediasi

Untuk informasi tentang penggunaan AWS Backup untuk sistem file EFS, lihat Men cadangkan sistem file EFS di Panduan Pengguna Sistem File Amazon Elastic.

[EFS.8] Sistem file EFS harus dienkripsi saat diam

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.3.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EFS::FileSystem`

AWS Config aturan: efs-filesystem-ct-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon EFS mengenkripsi data dengan AWS Key Management Service (AWS KMS). Kontrol gagal jika sistem file tidak dienkripsi.

Data diam mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi apa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengaktifkan enkripsi saat diam untuk sistem file EFS baru, lihat Men genkripsi data saat diam di Panduan Pengguna Sistem File Amazon Elastic.

Kontrol CSPM Hub Keamanan untuk Amazon EKS

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon Elastic Kubernetes Service (Amazon EKS). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EKS.1] Titik akhir cluster EKS tidak boleh diakses publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: eks-endpoint-no-public-access

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akhir cluster Amazon EKS dapat diakses publik. Kontrol gagal jika cluster EKS memiliki titik akhir yang dapat diakses publik.

Saat Anda membuat cluster baru, Amazon EKS membuat titik akhir untuk server API Kubernetes terkelola yang Anda gunakan untuk berkomunikasi dengan cluster Anda. Secara default, titik akhir server API ini tersedia untuk umum untuk internet. Akses ke server API diamankan menggunakan kombinasi AWS Identity and Access Management (IAM) dan Kubernetes Role Based Access Control

(RBAC) asli. Dengan menghapus akses publik ke titik akhir, Anda dapat menghindari paparan dan akses yang tidak disengaja ke cluster Anda.

Remediasi

Untuk memodifikasi akses titik akhir untuk cluster EKS yang ada, lihat Memodifikasi akses titik akhir cluster di Panduan Pengguna Amazon EKS . Anda dapat mengatur akses titik akhir untuk cluster EKS baru saat membuatnya. Untuk petunjuk cara membuat cluster Amazon EKS baru, lihat Membuat cluster Amazon EKS di Panduan Pengguna Amazon EKS .

[EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/12.3.4

Kategori: Identifikasi > Kerentanan, patch, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: eks-cluster-supported-version

Jenis jadwal: Perubahan dipicu

Parameter:

- `oldestVersionSupported`: `1.34` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah cluster Amazon Elastic Kubernetes Service (Amazon EKS) berjalan pada versi Kubernetes dukungan standar. Kontrol gagal jika cluster Amazon EKS berjalan pada versi dukungan yang tidak didukung atau diperpanjang.

Jika aplikasi Anda tidak memerlukan versi Kubernetes tertentu, sebaiknya gunakan versi Kubernetes terbaru yang tersedia yang didukung oleh EKS untuk cluster Anda. Untuk informasi selengkapnya, lihat kalender rilis Amazon EKS Kubernetes dan Mem ahami siklus hidup versi Kubernetes di Amazon EKS di Panduan Pengguna Amazon EKS.

Remediasi

Untuk memperbarui cluster EKS, lihat Memper barui cluster yang ada ke versi Kubernetes baru di Panduan Pengguna Amazon EKS.

[EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi

Persyaratan terkait: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, PCI DSS v4.0. 1/8.3.2

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: eks-cluster-secrets-encrypted

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon EKS menggunakan rahasia Kubernetes terenkripsi. Kontrol gagal jika rahasia Kubernetes cluster tidak dienkripsi.

Saat mengenkripsi rahasia, Anda dapat menggunakan kunci AWS Key Management Service (AWS KMS) untuk menyediakan enkripsi amplop rahasia Kubernetes yang disimpan di etcd untuk cluster Anda. Enkripsi ini merupakan tambahan untuk enkripsi volume EBS yang diaktifkan secara default untuk semua data (termasuk rahasia) yang disimpan di etcd sebagai bagian dari cluster EKS. Menggunakan enkripsi rahasia untuk cluster EKS Anda memungkinkan Anda menerapkan strategi pertahanan mendalam untuk aplikasi Kubernetes dengan mengenkripsi rahasia Kubernetes dengan kunci KMS yang Anda tentukan dan kelola.

> **Note**
>
> Kontrol ini akan dihentikan setelah 10 Agustus 2026 dan dihapus dari semua standar CSPM Security Hub yang berlaku. Dimulai dengan Kubernetes versi 1.28, cluster Amazon EKS memiliki rahasia Kubernetes yang dilindungi dengan enkripsi amplop secara default.

Remediasi

Untuk mengaktifkan enkripsi rahasia pada cluster EKS, lihat Mengaktifkan enkripsi rahasia pada cluster yang ada di Panduan Pengguna Amazon EKS .

[EKS.6] Cluster EKS harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: `tagged-eks-cluster` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah cluster Amazon EKS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke cluster EKS, lihat Men andai sumber daya Amazon EKS Anda di Panduan Pengguna Amazon EKS.

[EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::EKS::IdentityProviderConfig`

AWS Config aturan: `tagged-eks-identityproviderconfig` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah konfigurasi penyedia identitas Amazon EKS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika

konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke konfigurasi penyedia identitas EKS, lihat Men andai sumber daya Amazon EKS Anda di Panduan Pengguna Amazon EKS.

[EKS.8] Cluster EKS harus mengaktifkan logging audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7) NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EKS::Cluster`

AWS Config aturan: eks-cluster-log-enabled

Jenis jadwal: Perubahan dipicu

Parameter:

- `logTypes: audit`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah cluster Amazon EKS mengaktifkan pencatatan audit. Kontrol gagal jika pencatatan audit tidak diaktifkan untuk cluster.

> **Note**
>
> Kontrol ini tidak memeriksa apakah pencatatan audit Amazon EKS diaktifkan melalui Amazon Security Lake untuk Akun AWS.

Pencatatan pesawat kontrol EKS menyediakan log audit dan diagnostik langsung dari bidang kontrol EKS ke Amazon CloudWatch Log di akun Anda. Anda dapat memilih jenis log yang Anda butuhkan, dan log dikirim sebagai aliran log ke grup untuk setiap cluster EKS di CloudWatch. Logging memberikan visibilitas ke dalam akses dan kinerja cluster EKS. Dengan mengirimkan log pesawat kontrol EKS untuk cluster EKS Anda ke CloudWatch Log, Anda dapat merekam operasi untuk tujuan audit dan diagnostik di lokasi pusat.

Remediasi

Untuk mengaktifkan log audit untuk cluster EKS Anda, lihat Mengaktifkan dan menonaktifkan log bidang kontrol di Panduan Pengguna Amazon EKS .

[EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung

Kategori: Identifikasi > Kerentanan, patch, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EKS::Nodegroup`

AWS Config aturan: eks-nodegroup-supported-version-check

Jenis jadwal: Perubahan dipicu

Parameter:

- `oldestVersionSupported`: `1.34` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah grup simpul Amazon EKS berjalan pada versi Kubernetes dukungan standar. Kontrol gagal jika grup simpul Amazon EKS berjalan pada versi dukungan yang tidak didukung atau diperpanjang.

Menjalankan grup simpul EKS pada versi Kubernetes yang tidak didukung berarti node tersebut tidak lagi menerima tambalan keamanan, perbaikan bug, atau pembaruan kompatibilitas dari. AWS Versi yang tidak didukung mungkin berisi kerentanan yang diketahui yang telah diatasi dalam rilis yang lebih baru, dan mereka mungkin mengalami masalah kompatibilitas dengan gambar kontainer yang diperbarui Layanan AWS, dan alat pihak ketiga di ekosistem Kubernetes. Jika aplikasi Anda tidak memerlukan versi Kubernetes tertentu, sebaiknya gunakan versi Kubernetes terbaru yang tersedia yang didukung oleh Amazon EKS untuk grup node Anda. Untuk informasi selengkapnya, lihat kalender rilis Amazon EKS Kubernetes dan Memahami setiap fase pembaruan node di Panduan Pengguna Amazon EKS.

Remediasi

Untuk memperbarui grup simpul EKS, lihat Memperbarui grup node terkelola untuk cluster Anda di Panduan Pengguna Amazon EKS .

Kontrol CSPM Security Hub untuk ElastiCache

AWS Security Hub CSPMKontrol ini mengevaluasi ElastiCache layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Tinggi

Jenis sumber daya:`AWS::ElastiCache::CacheCluster`, `AWS:ElastiCache:ReplicationGroup`

AWS Configaturan: elasticache-redis-cluster-automatic-backup-check

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`snapshotRetentionPeriod`	Periode retensi snapshot minimum dalam beberapa hari	Bilangan Bulat	1 untuk 35	1

Kontrol ini mengevaluasi apakah klaster Amazon ElastiCache (Redis OSS) mengaktifkan pencadangan otomatis. Kontrol gagal jika `SnapshotRetentionLimit` untuk cluster Redis OSS kurang dari periode waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi snapshot, Security Hub CSPM menggunakan nilai default 1 hari.

ElastiCache (Redis OSS) cluster dapat mencadangkan data mereka. Anda dapat menggunakan backup untuk memulihkan klaster atau menyemai klaster baru. Cadangan terdiri dari metadata cluster, bersama dengan semua data di cluster. Semua cadangan ditulis ke Amazon S3, yang menyediakan penyimpanan tahan lama. Anda dapat memulihkan data Anda dengan membuat ElastiCache cluster baru dan mengisinya dengan data dari cadangan. Anda dapat mengelola backup menggunakanKonsol Manajemen AWS, theAWS CLI, dan API. ElastiCache

> **Note**
>
> Kontrol ini juga mengevaluasi kelompok replikasi ElastiCache (Redis OSS dan Valkey).

Remediasi

Untuk informasi tentang penjadwalan pencadangan otomatis untuk ElastiCache klaster, lihat Menjadwalkan pencadangan otomatis di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5) PCI DSS v4.0. 1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElastiCache::CacheCluster`

AWS Configaturan: elasticache-auto-minor-version-upgrade-check

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah Amazon ElastiCache secara otomatis menerapkan upgrade versi minor ke cluster cache. Kontrol gagal jika cluster cache tidak memiliki upgrade versi minor yang diterapkan secara otomatis.

> **Note**
>
> Kontrol ini tidak berlaku untuk cluster ElastiCache Memcached.

Upgrade versi minor otomatis adalah fitur yang dapat Anda aktifkan di Amazon ElastiCache untuk secara otomatis meningkatkan cluster cache Anda ketika versi mesin cache minor baru tersedia. Upgrade ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up-to-date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk secara otomatis menerapkan upgrade versi minor ke cluster ElastiCache cache yang ada, lihat Pengelolaan versi untuk ElastiCache di Panduan ElastiCache Pengguna Amazon.

[ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 SC-36,, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Configaturan: elasticache-repl-grp-auto-failover-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup ElastiCache replikasi mengaktifkan failover otomatis. Kontrol gagal jika failover otomatis tidak diaktifkan untuk grup replikasi.

Ketika failover otomatis diaktifkan untuk grup replikasi, peran node utama akan secara otomatis gagal ke salah satu replika baca. Promosi failover dan replika ini memastikan bahwa Anda dapat melanjutkan penulisan ke primer baru setelah promosi selesai, yang mengurangi waktu henti secara keseluruhan jika terjadi kegagalan.

Remediasi

Untuk mengaktifkan failover otomatis untuk grup ElastiCache replikasi yang ada, lihat Memodifikasi ElastiCache klaster di Panduan Pengguna Amazon ElastiCache . Jika Anda menggunakan ElastiCache konsol, setel Auto failover ke diaktifkan.

[ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Configaturan: elasticache-repl-grp-encrypted-at-rest

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup ElastiCache replikasi dienkripsi saat istirahat. Kontrol gagal jika grup replikasi tidak dienkripsi saat istirahat.

Mengenkripsi data saat istirahat mengurangi risiko bahwa pengguna yang tidak diautentikasi mendapatkan akses ke data yang disimpan pada disk. ElastiCache (Redis OSS) grup replikasi harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Untuk mengonfigurasi enkripsi saat istirahat pada grup ElastiCache replikasi, lihat Mengaktifkan enkripsi saat istirahat di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Configaturan: elasticache-repl-grp-encrypted-in-transit

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup ElastiCache replikasi dienkripsi dalam perjalanan. Kontrol gagal jika grup replikasi tidak dienkripsi saat transit.

Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan. Mengaktifkan enkripsi dalam transit pada grup ElastiCache replikasi mengenkripsi data Anda setiap kali data berpindah dari satu tempat ke tempat lain, seperti antar node di cluster Anda atau antara cluster Anda dan aplikasi Anda.

Remediasi

Untuk mengonfigurasi enkripsi dalam transit pada grup ElastiCache replikasi, lihat Mengaktifkan enkripsi dalam transit di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, PCI DSS v4.0. 1/8.3.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElastiCache::ReplicationGroup`

AWS Configaturan: elasticache-repl-grp-redis-auth-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup replikasi ElastiCache (Redis OSS) mengaktifkan Redis OSS AUTH. Kontrol gagal jika versi Redis OSS dari node grup replikasi di bawah 6.0 dan `AuthToken` tidak digunakan.

Saat Anda menggunakan token otentikasi Redis, atau kata sandi, Redis memerlukan kata sandi sebelum mengizinkan klien menjalankan perintah, yang meningkatkan keamanan data. Untuk Redis 6.0 dan versi yang lebih baru, sebaiknya gunakan Role-Based Access Control (RBAC). Karena RBAC tidak didukung untuk versi Redis lebih awal dari 6.0, kontrol ini hanya mengevaluasi versi yang tidak dapat menggunakan fitur RBAC.

Remediasi

Untuk menggunakan Redis AUTH pada grup replikasi ElastiCache (Redis OSS), lihat Memodifikasi token AUTH pada klaster ElastiCache (Redis OSS) yang ada di Panduan Pengguna Amazon. ElastiCache

[ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElastiCache::CacheCluster`

AWS Configaturan: elasticache-subnet-group-check

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah ElastiCache cluster dikonfigurasi dengan grup subnet kustom. Kontrol gagal jika `CacheSubnetGroupName` untuk ElastiCache cluster memiliki nilai`default`.

Saat meluncurkan ElastiCache cluster, grup subnet default dibuat jika belum ada. Grup default menggunakan subnet dari Virtual Private Cloud (VPC) default. Sebaiknya gunakan grup subnet khusus yang lebih membatasi subnet tempat cluster berada, dan jaringan yang diwarisi cluster dari subnet.

Remediasi

Untuk membuat grup subnet baru untuk ElastiCache klaster, lihat Membuat grup subnet di ElastiCache Panduan Pengguna Amazon.

Kontrol CSPM Security Hub untuk Elastic Beanstalk

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Elastic Beanstalk layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ElasticBeanstalk::Environment`

AWS Configaturan: **`beanstalk-enhanced-health-reporting-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pelaporan kesehatan yang ditingkatkan diaktifkan untuk AWS Elastic Beanstalk lingkungan Anda.

Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk memungkinkan respons yang lebih cepat terhadap perubahan kesehatan infrastruktur yang mendasarinya. Perubahan ini dapat mengakibatkan kurangnya ketersediaan aplikasi.

Pelaporan kesehatan yang ditingkatkan Elastic Beanstalk menyediakan deskriptor status untuk mengukur tingkat keparahan masalah yang diidentifikasi dan mengidentifikasi kemungkinan penyebab untuk diselidiki. Agen kesehatan Elastic Beanstalk, termasuk dalam Amazon Machine Images (AMI) yang didukung, mengevaluasi log dan metrik instans EC2 lingkungan.

Untuk informasi tambahan, lihat Pelaporan dan pemantauan kesehatan yang ditingkatkan di Panduan AWS Elastic Beanstalk Pengembang.

Remediasi

Untuk petunjuk tentang cara mengaktifkan pelaporan kesehatan yang disempurnakan, lihat Mengaktifkan pelaporan kesehatan yang disempurnakan menggunakan konsol Elastic Beanstalk di Panduan Pengembang. AWS Elastic Beanstalk

[ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElasticBeanstalk::Environment`

AWS Configaturan: **`elastic-beanstalk-managed-updates-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`UpdateLevel`	Tingkat pembaruan versi	Enum	`minor`, `patch`	Tidak ada nilai default

Kontrol ini memeriksa apakah pembaruan platform terkelola diaktifkan untuk lingkungan Elastic Beanstalk. Kontrol gagal jika tidak ada pembaruan platform terkelola yang diaktifkan. Secara default, kontrol lolos jika semua jenis pembaruan platform diaktifkan. Secara opsional, Anda dapat memberikan nilai parameter khusus untuk memerlukan tingkat pembaruan tertentu.

Mengaktifkan pembaruan platform terkelola memastikan bahwa perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan diinstal. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk mengaktifkan pembaruan platform terkelola, lihat Untuk mengonfigurasi pembaruan platform terkelola di bawah Pembaruan platform terkelola di Panduan AWS Elastic Beanstalk Pengembang.

[ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

Persyaratan terkait: PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::ElasticBeanstalk::Environment`

AWS Configaturan: **`elastic-beanstalk-logs-to-cloudwatch`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`RetentionInDays`	Jumlah hari untuk menyimpan peristiwa log sebelum kedaluwarsa	Enum	`1`, `3`, `5`, `7`, `14`, `30`, `60`, `90`, `120`, `150`, `180`, `365` , `400`, `545`, `731`, `1827`, `3653`	Tidak ada nilai default

Kontrol ini memeriksa apakah lingkungan Elastic Beanstalk dikonfigurasi untuk mengirim log ke Log. CloudWatch Kontrol gagal jika lingkungan Elastic Beanstalk tidak dikonfigurasi untuk mengirim log ke Log. CloudWatch Secara opsional, Anda dapat memberikan nilai kustom untuk `RetentionInDays` parameter jika Anda ingin kontrol lulus hanya jika log dipertahankan untuk jumlah hari yang ditentukan sebelum kedaluwarsa.

CloudWatch membantu Anda mengumpulkan dan memantau berbagai metrik untuk aplikasi dan sumber daya infrastruktur Anda. Anda juga dapat menggunakan CloudWatch untuk mengonfigurasi tindakan alarm berdasarkan metrik tertentu. Sebaiknya integrasikan Elastic Beanstalk dengan Elastic CloudWatch Beanstalk untuk meningkatkan visibilitas ke lingkungan Elastic Beanstalk Anda. Log Elastic Beanstalk mencakup eb-activity.log, log akses dari server proxy nginx atau Apache lingkungan, dan log yang khusus untuk lingkungan.

Remediasi

Untuk mengintegrasikan Elastic CloudWatch Beanstalk dengan Log, lihat Streaming CloudWatch log instance ke Log di Panduan Pengembang. AWS Elastic Beanstalk

Kontrol CSPM Hub Keamanan untuk Penyeimbangan Beban Elastis

AWS Security Hub CSPM Kontrol ini mengevaluasi layanan dan sumber daya Elastic Load Balancing. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS

Persyaratan terkait: PCI DSS v3.2. 1/2.3, PCI DSS v3.2. 1/4.1, NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: alb-http-to-https-redirection-check

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengalihan HTTP ke HTTPS dikonfigurasi pada semua pendengar HTTP dari Application Load Balancers. Kontrol gagal jika salah satu pendengar HTTP dari Application Load Balancers tidak mengonfigurasi pengalihan HTTP ke HTTPS.

Sebelum mulai menggunakan Application Load Balancer, Anda harus menambahkan satu atau lebih pendengar. Listener adalah proses yang menggunakan protokol dan port yang dikonfigurasi untuk memeriksa permintaan koneksi. Pendengar mendukung protokol HTTP dan HTTPS. Anda dapat menggunakan pendengar HTTPS untuk menurunkan pekerjaan enkripsi dan dekripsi ke penyeimbang beban Anda. Untuk menerapkan enkripsi saat transit, Anda harus menggunakan tindakan pengalihan dengan Application Load Balancers untuk mengarahkan permintaan HTTP klien ke permintaan HTTPS di port 443.

Untuk mempelajari selengkapnya, lihat Pen dengar untuk Penyeimbang Beban Aplikasi Anda di Panduan Pengguna untuk Penyeimbang B eban Aplikasi.

Remediasi

Untuk mengalihkan permintaan HTTP ke HTTPS, Anda harus menambahkan aturan pendengar Application Load Balancer atau mengedit aturan yang ada.

Untuk petunjuk tentang menambahkan aturan baru, lihat Men ambahkan aturan di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk Protocol: Port, pilih HTTP, lalu masukkan**80**. Untuk Tambah tindakan, Arahkan kembali ke, pilih HTTPS, lalu masukkan**443**.

Untuk petunjuk tentang mengedit aturan yang ada, lihat Meng edit aturan di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk Protocol: Port, pilih HTTP, lalu masukkan**80**. Untuk Tambah tindakan, Arahkan kembali ke, pilih HTTPS, lalu masukkan**443**.

[ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (5), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: elb-acm-certificate-required

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Classic Load Balancer menggunakan HTTPS/SSL sertifikat yang disediakan oleh AWS Certificate Manager (ACM). Kontrol gagal jika Classic Load Balancer yang dikonfigurasi dengan HTTPS/SSL pendengar tidak menggunakan sertifikat yang disediakan oleh ACM.

Untuk membuat sertifikat, Anda dapat menggunakan ACM atau alat yang mendukung protokol SSL dan TLS, seperti OpenSSL. Security Hub CSPM merekomendasikan agar Anda menggunakan ACM untuk membuat atau mengimpor sertifikat untuk penyeimbang beban Anda.

ACM terintegrasi dengan Classic Load Balancers sehingga Anda dapat menerapkan sertifikat pada penyeimbang beban Anda. Anda juga harus memperbarui sertifikat ini secara otomatis.

Remediasi

Untuk informasi tentang cara mengaitkan SSL/TLS sertifikat ACM dengan Classic Load Balancer, lihat artikel Pusat Penget AWS ahuan Bagaimana cara mengaitkan SSL/TLS sertifikat ACM dengan Classic, Application, atau Network Load Balancer?

[ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4),, (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: elb-tls-https-listeners-only

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pendengar Classic Load Balancer Anda dikonfigurasi dengan protokol HTTPS atau TLS untuk koneksi front-end (client to load balancer). Kontrol ini berlaku jika Classic Load Balancer memiliki pendengar. Jika Classic Load Balancer Anda tidak memiliki pendengar yang dikonfigurasi, maka kontrol tidak melaporkan temuan apa pun.

Kontrol akan lolos jika pendengar Classic Load Balancer dikonfigurasi dengan TLS atau HTTPS untuk koneksi front-end.

Kontrol gagal jika pendengar tidak dikonfigurasi dengan TLS atau HTTPS untuk koneksi front-end.

Sebelum Anda mulai menggunakan penyeimbang beban, Anda harus menambahkan satu atau lebih pendengar. Listener adalah proses yang menggunakan protokol dan port yang dikonfigurasi untuk memeriksa permintaan koneksi. Pendengar dapat mendukung HTTP dan HTTPS/TLS protokol. Anda harus selalu menggunakan pendengar HTTPS atau TLS, sehingga penyeimbang beban melakukan pekerjaan enkripsi dan dekripsi saat transit.

Remediasi

Untuk mengatasi masalah ini, perbarui pendengar Anda untuk menggunakan protokol TLS atau HTTPS.

Untuk mengubah semua pendengar yang tidak patuh menjadi TLS/HTTPS pendengar

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.

2. Pada panel navigasi, di bawah Penyeimbangan Beban, pilih Penyeimbang Beban.
3. Pilih Classic Load Balancer Anda.
4. Pada tab Pen dengar, pilih Edit.
5. Untuk semua pendengar di mana Load Balancer Protocol tidak disetel ke HTTPS atau SSL, ubah setelan ke HTTPS atau SSL.
6. Untuk semua pendengar yang dimodifikasi, pada tab Sertifikat, pilih Ubah default.
7. Untuk sertifikat ACM dan IAM, pilih sertifikat.
8. Pilih Simpan sebagai default.
9. Setelah Anda memperbarui semua pendengar, pilih S impan.

[ELB.4] Application Load Balancer harus dikonfigurasi untuk menghapus header http yang tidak valid

Persyaratan terkait: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/6.2.4

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: alb-http-drop-invalid-header-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah Application Load Balancer dikonfigurasi untuk menghapus header HTTP yang tidak valid. Kontrol gagal jika nilai `routing.http.drop_invalid_header_fields.enabled` diatur ke`false`.

Secara default, Application Load Balancers tidak dikonfigurasi untuk menghapus nilai header HTTP yang tidak valid. Menghapus nilai header ini mencegah serangan desync HTTP.

> **Note**
>
> Sebaiknya nonaktifkan kontrol ini jika ELB.12 diaktifkan di akun Anda. Untuk informasi selengkapnya, lihat [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat.

Remediasi

Untuk mengatasi masalah ini, konfigurasikan penyeimbang beban Anda untuk menghapus bidang header yang tidak valid.

Untuk mengonfigurasi penyeimbang beban untuk menghapus bidang header yang tidak valid

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, pilih Load penyeimbang.
3. Pilih Penyeimbang Beban Aplikasi.
4. Dari T ind akan, pilih Edit atribut.
5. Di bawah J atuhkan Bidang Header Tidak Valid, pilih Aktifkan.
6. Pilih Simpan.

[ELB.5] Aplikasi dan pencatatan Penyeimbang Beban Klasik harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: elb-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application Load Balancer dan Classic Load Balancer telah mengaktifkan logging. Kontrol gagal jika `access_logs.s3.enabled` ada`false`.

Elastic Load Balancing memberikan log akses yang mengambil informasi mendetail tentang permintaan yang dikirim ke penyeimbang beban Anda. Setiap log berisi informasi, seperti waktu

permintaan diterima, alamat IP klien, latensi, jalur permintaan, dan respons server. Anda dapat menggunakan log akses ini untuk menganalisis pola lalu lintas dan memecahkan masalah.

Untuk mempelajari selengkapnya, lihat Log Akses untuk Penyeimbang Beban Klasik Anda di Panduan Pengguna untuk Penyeimbang B eban Klasik.

Remediasi

Untuk mengaktifkan log akses, lihat Langkah 3: Mengkonfigurasi log akses di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

[ELB.6] Aplikasi, Gateway, dan Penyeimbang Beban Jaringan harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: elb-deletion-protection-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Aplikasi, Gateway, atau Network Load Balancer mengaktifkan perlindungan penghapusan. Kontrol gagal jika perlindungan penghapusan dinonaktifkan.

Aktifkan perlindungan penghapusan untuk melindungi Aplikasi, Gateway, atau Network Load Balancer Anda dari penghapusan.

Remediasi

Untuk mencegah penyeimbang beban terhapus secara tidak sengaja, Anda dapat mengaktifkan perlindungan penghapusan. Secara default, perlindungan penghapusan dinonaktifkan untuk penyeimbang beban Anda.

Jika Anda mengaktifkan perlindungan penghapusan untuk penyeimbang beban, Anda harus menonaktifkan perlindungan hapus sebelum Anda dapat menghapus penyeimbang beban.

Untuk mengaktifkan perlindungan penghapusan untuk Penyeimbang Beban Aplikasi, lihat Perlindungan penghapusan di Panduan Pengguna untuk Penyeimbang B eban Aplikasi. Untuk mengaktifkan perlindungan penghapusan untuk Gateway Load Balancer, lihat Perlindungan penghapusan di Panduan Pengguna untuk Penyeimbang B eban Gateway. Untuk mengaktifkan perlindungan penghapusan untuk Network Load Balancer, lihat Perlindungan penghapusan di Panduan Pengguna untuk Penyeimbang B eban Jaringan.

[ELB.7] Classic Load Balancer harus mengaktifkan pengeringan koneksi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Puli hkan > Ketahanan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: `elb-connection-draining-enabled` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Classic Load Balancers mengaktifkan pengeringan koneksi.

Mengaktifkan pengeringan koneksi pada Classic Load Balancers memastikan bahwa penyeimbang beban berhenti mengirim permintaan ke instans yang tidak registrasi atau tidak sehat. Itu membuat koneksi yang ada tetap terbuka. Ini sangat berguna untuk contoh di grup Penskalaan Otomatis, untuk memastikan bahwa koneksi tidak terputus secara tiba-tiba.

Remediasi

Untuk mengaktifkan pengeringan koneksi pada Classic Load Balancer, lihat Meng onfigurasi pengeringan koneksi untuk Classic Load Balancer Anda di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki kekuatan AWS Config urasi

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3),

NIST.800-53.r5 SC-7 (4),, (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0. 1/4.2.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: elb-predefined-security-policy-ssl-check

Jenis jadwal: Perubahan dipicu

Parameter:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah HTTPS/SSL pendengar Classic Load Balancer menggunakan kebijakan `ELBSecurityPolicy-TLS-1-2-2017-01` yang telah ditentukan sebelumnya. Kontrol gagal jika pen HTTPS/SSL dengar Classic Load Balancer tidak menggunakan`ELBSecurityPolicy-TLS-1-2-2017-01`.

Kebijakan keamanan adalah kombinasi dari protokol SSL, cipher, dan opsi Server Order Preference. Kebijakan yang telah ditentukan mengontrol sandi, protokol, dan perintah preferensi untuk didukung selama negosiasi SSL antara klien dan penyeimbang beban.

Menggunakan `ELBSecurityPolicy-TLS-1-2-2017-01` dapat membantu Anda memenuhi standar kepatuhan dan keamanan yang mengharuskan Anda menonaktifkan versi SSL dan TLS tertentu. Untuk informasi selengkapnya, lihat Kebijakan keamanan SSL yang telah ditetapkan untuk Penyeimbang Beban Klasik di Panduan Pengguna untuk Penyeimbang B eban Klasik.

Remediasi

Untuk informasi tentang cara menggunakan kebijakan keamanan yang telah ditentukan sebelumnya `ELBSecurityPolicy-TLS-1-2-2017-01` dengan Classic Load Balancer, lihat Meng onfigurasi pengaturan keamanan di Panduan Pengguna untuk Penyeimbang B eban Klasik.

[ELB.9] Penyeimbang Beban Klasik harus mengaktifkan penyeimbangan beban lintas zona

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: elb-cross-zone-load-balancing-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penyeimbangan beban lintas zona diaktifkan untuk Classic Load Balancers (CLB). Kontrol gagal jika penyeimbangan beban lintas zona tidak diaktifkan untuk CLB.

Node penyeimbang beban mendistribusikan lalu lintas hanya di seluruh target terdaftar di Zona Ketersediaan. Ketika load balancing lintas zona dinonaktifkan, setiap node Load Balancer mendistribusikan lalu lintas hanya di target yang telah terdaftar di Availability Zonenya. Jika jumlah target terdaftar tidak sama di seluruh Zona Ketersediaan, lalu lintas tidak akan didistribusikan secara merata dan instance di satu zona mungkin akhirnya digunakan secara berlebihan dibandingkan dengan instance di zona lain. Dengan penyeimbangan beban lintas zona diaktifkan, setiap node penyeimbang beban untuk Classic Load Balancer Anda mendistribusikan permintaan secara merata di seluruh instans terdaftar di semua Availability Zone yang diaktifkan. Untuk detailnya, lihat Cross-zone penyeimbangan beban di Panduan Pengguna Elastic Load Balancing.

Remediasi

Untuk mengaktifkan penyeimbangan beban lintas zona di Classic Load Balancer, lihat Mengaktifkan penyeim bangan beban lintas zona di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: clb-multiple-az

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`minAvailabilityZones`	Jumlah Zona Ketersediaan Minimum	Enum	`2, 3, 4, 5, 6`	2

Kontrol ini memeriksa apakah Classic Load Balancer telah dikonfigurasi untuk menjangkau setidaknya jumlah Zona Ketersediaan (AZ) yang ditentukan. Kontrol gagal jika Classic Load Balancer tidak menjangkau setidaknya jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub CSPM menggunakan nilai default dua AZ.

Classic Load Balancer dapat diatur untuk mendistribusikan permintaan masuk di seluruh instans Amazon EC2 dalam satu Availability Zone atau beberapa Availability Zone. Penyeimbang Beban Klasik yang tidak menjangkau beberapa Zona Ketersediaan tidak dapat mengarahkan lalu lintas ke target di Zona Ketersediaan lain jika Zona Ketersediaan tunggal yang dikonfigurasi menjadi tidak tersedia.

Remediasi

Untuk menambahkan Zona Ketersediaan ke Penyeimbang Beban Klasik, lihat Men ambahkan atau menghapus subnet untuk Penyeimbang Beban Klasik Anda di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/6.2.4

Kategori: Mel indungi > Perlindungan Data > Integritas data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: alb-desync-mode-check

Jenis jadwal: Perubahan dipicu

Parameter:

- `desyncMode`: `defensive, strictest` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Application Load Balancer dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat. Kontrol gagal jika Application Load Balancer tidak dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat.

Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi rentan terhadap antrian permintaan atau keracunan cache. Pada gilirannya, kerentanan ini dapat menyebabkan pengisian kredensi atau eksekusi perintah yang tidak sah. Application Load Balancers yang dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat melindungi aplikasi Anda dari masalah keamanan yang mungkin disebabkan oleh HTTP Desync.

Remediasi

Untuk memperbarui mode mitigasi desync dari Penyeimbang Beban Aplikasi, lihat Mode mitigasi Desync di Panduan Pengguna untuk Penyeimbang Beban Aplikasi.

[ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: elbv2-multiple-az

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`minAvailabilityZones`	Jumlah Zona Ketersediaan Minimum	Enum	`2, 3, 4, 5, 6`	2

Kontrol ini memeriksa apakah Elastic Load Balancer V2 (Application, Network, atau Gateway Load Balancer) telah mendaftarkan instans dari setidaknya jumlah Availability Zone (AZ) yang ditentukan. Kontrol gagal jika Elastic Load Balancer V2 tidak memiliki instans terdaftar setidaknya dalam jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub CSPM menggunakan nilai default dua AZ.

Elastic Load Balancing secara otomatis mendistribusikan lalu lintas aplikasi masuk di beberapa target, seperti instans EC2, wadah, dan IP addresses, dalam satu atau lebih Zona Ketersediaan. Elastic Load Balancing menskalakan load balancer Anda saat lalu lintas masuk Anda berubah seiring waktu. Disarankan untuk mengonfigurasi setidaknya dua zona ketersediaan untuk memastikan ketersediaan layanan, karena Elastic Load Balancer akan dapat mengarahkan lalu lintas ke zona ketersediaan lain jika salah satu tidak tersedia. Memiliki beberapa zona ketersediaan yang dikonfigurasi akan membantu menghilangkan satu titik kegagalan untuk aplikasi.

Remediasi

Untuk menambahkan Zona Ketersediaan ke Penyeimbang Beban Aplikasi, lihat Zona Keter sediaan untuk Penyeimbang Beban Aplikasi Anda di Panduan Pengguna untuk Penyeimbang Beban Aplikasi. Untuk menambahkan Zona Ketersediaan ke Penyeimbang Beban Jaringan, lihat Penyeimbang B eban Jaringan di Panduan Pengguna untuk Penyeimbang Beban Jaringan. Untuk menambahkan Zona Ketersediaan ke Gateway Load Balancer, lihat Membuat Penyeimbang Beban Gateway di Panduan Pengguna untuk Penyeimbang Beban Gateway.

[ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/6.2.4

Kategori: Mel indungi > Perlindungan Data > Integritas data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config aturan: clb-desync-mode-check

Jenis jadwal: Perubahan dipicu

Parameter:

- `desyncMode`: `defensive, strictest` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah Classic Load Balancer dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat. Kontrol gagal jika Classic Load Balancer tidak dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat.

Masalah HTTP Desync dapat menyebabkan penyelundupan permintaan dan membuat aplikasi rentan terhadap antrian permintaan atau keracunan cache. Pada gilirannya, kerentanan ini dapat menyebabkan pembajakan kredensi atau eksekusi perintah yang tidak sah. Classic Load Balancers yang dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat melindungi aplikasi Anda dari masalah keamanan yang mungkin disebabkan oleh HTTP Desync.

Remediasi

Untuk memperbarui mode mitigasi desync pada Classic Load Balancer, lihat Memodi fikasi mode mitigasi desync di Panduan Pengguna untuk Penyeimbang Beban Klasik.

[ELB.16] Penyeimbang Beban Aplikasi harus dikaitkan dengan AWS WAF ACL web

Persyaratan terkait: NIST.800-53.r5 AC-4 (21)

Kategori: Melindungi > Layanan perlindungan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config aturan: alb-waf-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Application Load Balancer dikaitkan dengan daftar kontrol akses AWS WAF klasik atau AWS WAF web (ACL web). Kontrol gagal jika `Enabled` bidang untuk AWS WAF konfigurasi disetel ke`false`.

AWS WAF adalah firewall aplikasi web yang membantu melindungi aplikasi web dan API dari serangan. Dengan AWS WAF, Anda dapat mengonfigurasi ACL web, yang merupakan sekumpulan aturan yang mengizinkan, memblokir, atau menghitung permintaan web berdasarkan aturan dan kondisi keamanan web yang dapat disesuaikan yang Anda tetapkan. Sebaiknya kaitkan Application Load Balancer Anda dengan ACL AWS WAF web untuk membantu melindunginya dari serangan berbahaya.

Remediasi

Untuk mengaitkan Application Load Balancer dengan ACL web, lihat Meng asosiasikan atau memisahkan ACL web dengan sumber daya di Panduan Peng AWS embang. AWS WAF

[ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan

Persyaratan terkait: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4,, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23,, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::Listener`

AWS Config aturan: elbv2-predefined-security-policy-ssl-check

Jenis jadwal: Perubahan dipicu

Parameter: `sslPolicies`: `ELBSecurityPolicy-TLS13-1-3-2021-06, ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-2021-06, ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04, ELBSecurityPolicy-TLS13-1-2-Res-PQ-2025-09, ELBSecurityPolicy-`

`TLS13-1-3-PQ-2025-09`, `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-PQ-2025-09`, `ELBSecurityPolicy-TLS13-1-3-FIPS-PQ-2025-09` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pendengar HTTPS untuk Application Load Balancer atau pendengar TLS untuk Network Load Balancer dikonfigurasi untuk mengenkripsi data yang sedang transit dengan menggunakan kebijakan keamanan yang disarankan. Kontrol gagal jika pendengar HTTPS atau TLS untuk penyeimbang beban tidak dikonfigurasi untuk menggunakan kebijakan keamanan yang direkomendasikan.

Elastic Load Balancing menggunakan konfigurasi negosiasi SSL, yang dikenal sebagai kebijakan keamanan, untuk menegosiasikan koneksi antara klien dan penyeimbang beban. Kebijakan keamanan menentukan kombinasi protokol dan cipher. Protokol membuat koneksi aman antara klien dan server. Sandi adalah algoritme enkripsi yang menggunakan kunci enkripsi untuk membuat pesan kode. Selama proses negosiasi koneksi, klien dan penyeimbang beban menyajikan daftar sandi dan protokol yang masing-masing mendukung, dalam urutan preferensi. Menggunakan kebijakan keamanan yang direkomendasikan untuk penyeimbang beban dapat membantu Anda memenuhi standar kepatuhan dan keamanan.

Remediasi

Untuk informasi tentang kebijakan keamanan yang direkomendasikan dan cara memperbarui pendengar, lihat bagian berikut dari Panduan Pengguna Penyeimbangan Beban Elastis: Kebijakan keamanan untuk Penyeimbang Beban Aplikasi, Kebijakan keamanan untuk Penyeimbang Beban Jaringan, Memper barui pendengar HTTPS untuk Penyeimbang Beban Aplikasi Anda, dan Per barui pendengar untuk Penyeimbang Beban Jaringan Anda.

[ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::Listener`

AWS Config aturan: elbv2-listener-encryption-in-transit

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pendengar untuk Application Load Balancer atau Network Load Balancer dikonfigurasi untuk menggunakan protokol aman untuk enkripsi data dalam transit. Kontrol gagal jika pendengar Application Load Balancer tidak dikonfigurasi untuk menggunakan protokol HTTPS, atau pendengar Network Load Balancer tidak dikonfigurasi untuk menggunakan protokol TLS.

Untuk mengenkripsi data yang ditransmisikan antara klien dan penyeimbang beban, pendengar Elastic Load Balancer harus dikonfigurasi untuk menggunakan protokol keamanan standar industri: HTTPS untuk Penyeimbang Beban Aplikasi, atau TLS untuk Penyeimbang Beban Jaringan. Jika tidak, data yang dikirimkan antara klien dan penyeimbang beban rentan terhadap intersepsi, gangguan, dan akses tidak sah. Penggunaan HTTPS atau TLS oleh pendengar sejalan dengan praktik terbaik keamanan dan membantu memastikan kerahasiaan dan integritas data selama transmisi. Ini sangat penting untuk aplikasi yang menangani informasi sensitif, atau harus mematuhi standar keamanan yang memerlukan enkripsi data dalam transit.

Remediasi

Untuk informasi tentang mengonfigurasi protokol keamanan untuk pendengar, lihat bagian berikut dari Panduan Pengguna Elastic Load Balancing: Membuat pendengar HTTPS untuk Penyeimbang Beban Aplikasi dan Membuat pendengar untuk Penyeimbang B eban Jaringan Anda.

[ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config aturan: elbv2-targetgroup-healthcheck-protocol-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kelompok target untuk pemeriksaan kesehatan penyeimbang beban aplikasi dan jaringan menggunakan protokol transportasi terenkripsi. Kontrol gagal jika protokol pemeriksaan kesehatan tidak menggunakan HTTPS. Kontrol ini tidak berlaku untuk tipe target Lambda.

Load Balancer mengirim permintaan pemeriksaan kesehatan ke target terdaftar untuk menentukan status dan rute lalu lintas yang sesuai. Protokol pemeriksaan kesehatan yang ditentukan dalam konfigurasi kelompok target menentukan bagaimana pemeriksaan ini dilakukan. Ketika protokol pemeriksaan kesehatan menggunakan komunikasi yang tidak terenkripsi seperti HTTP, permintaan dan tanggapan dapat dicegat atau dimanipulasi selama transmisi. Hal ini memungkinkan penyerang mendapatkan wawasan tentang konfigurasi infrastruktur, merusak hasil pemeriksaan kesehatan, atau melakukan serangan man-in-the-middle yang memengaruhi keputusan routing. Menggunakan HTTPS untuk pemeriksaan kesehatan menyediakan komunikasi terenkripsi antara load balancer dan targetnya, melindungi integritas dan kerahasiaan informasi status kesehatan.

Remediasi

Untuk mengonfigurasi pemeriksaan kesehatan terenkripsi untuk grup target Penyeimbang Beban Aplikasi Anda, lihat Memper barui setelan pemeriksaan kesehatan grup target Penyeimbang Beban Aplikasi di Panduan Pengguna Penyeimbangan Beban Elastis. Untuk mengonfigurasi pemeriksaan kesehatan terenkripsi untuk grup target Network Load Balancer, lihat Memper barui setelan pemeriksaan kesehatan grup target Network Load Balancer di Panduan Pengguna Elastic Load Balancer.

[ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config aturan: elbv2-targetgroup-protocol-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kelompok target Elastic Load Balancing menggunakan protokol transport terenkripsi. Kontrol ini tidak berlaku untuk kelompok target dengan tipe target Lambda atau ALB, atau kelompok target menggunakan protokol GENEVE. Kontrol gagal jika kelompok target tidak menggunakan protokol HTTPS, TLS, atau QUIC.

Mengenkripsi data dalam perjalanan melindunginya dari intersepsi oleh pengguna yang tidak sah. Kelompok target yang menggunakan protokol tidak terenkripsi (HTTP, TCP, UDP) mengirimkan data tanpa enkripsi, membuatnya rentan terhadap penyadapan. Menggunakan protokol terenkripsi

(HTTPS, TLS, QUIC) memastikan bahwa data yang dikirimkan antara penyeimbang beban dan target dilindungi.

Remediasi

Untuk menggunakan protokol terenkripsi, Anda harus membuat grup target baru dengan protokol HTTPS, TLS, atau QUIC. Protokol kelompok target tidak dapat dimodifikasi setelah pembuatan. Untuk membuat grup target Penyeimbang Beban Aplikasi, lihat Membuat grup target untuk Penyeimbang Beban Aplikasi Anda di Panduan Pengguna Elastic Load Balancing. Untuk membuat grup target Network Load Balancer, lihat Membuat grup target untuk Network Load Balancer Anda di Panduan Pengguna Elastic Load Balancing.

Hub Keamanan CSPM untuk Elasticsearch

AWS Security Hub CSPM Kontrol ini mengevaluasi layanan dan sumber daya Elasticsearch.

Kontrol ini mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: PCI DSS v3.2. 1/3.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-encrypted-at-rest`

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan konfigurasi enkripsi saat istirahat. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan.

Untuk lapisan keamanan tambahan untuk data sensitif Anda OpenSearch, Anda harus mengonfigurasi OpenSearch agar dienkripsi saat diam. Domain Elasticsearch menawarkan enkripsi

data saat istirahat. Fitur ini digunakan AWS KMS untuk menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, ia menggunakan algoritma Advanced Encryption Standard dengan kunci 256-bit ()AES-256.

Untuk mempelajari lebih lanjut tentang OpenSearch enkripsi saat diam, lihat Enkripsi data diam untuk OpenSearch Layanan Amazon di Panduan Pengembang OpenSearch Layanan Amazon.

Jenis instans tertentu, seperti `t.small` dan`t.medium`, tidak mendukung enkripsi data saat diam. Untuk detailnya, lihat Jenis instans yang didukung di Panduan Pengembang OpenSearch Layanan Amazon.

Remediasi

Untuk mengaktifkan enkripsi saat diam untuk domain Elasticsearch baru dan yang sudah ada, lihat Meng aktifkan enkripsi data diam di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya dalam VPC

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-in-vpc-only`

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch berada di VPC. Itu tidak mengevaluasi konfigurasi routing subnet VPC untuk menentukan akses publik. Anda harus memastikan bahwa domain Elasticsearch tidak dilampirkan ke subnet publik. Lihat Resource-based kebijakan di

Panduan Pengembang OpenSearch Layanan Amazon. Anda juga harus memastikan bahwa VPC Anda dikonfigurasi sesuai dengan praktik terbaik yang disarankan. Lihat Praktik terbaik Keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

Domain Elasticsearch yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data yang sedang transit. VPC menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke domain Elasticsearch, termasuk ACL jaringan dan grup keamanan. Security Hub CSPM merekomendasikan agar Anda memigrasikan domain Elasticsearch publik ke VPC untuk memanfaatkan kontrol ini.

Remediasi

Jika Anda membuat domain dengan titik akhir publik, nanti Anda tidak dapat menempatkannya dalam VPC. Sebagai gantinya, Anda harus membuat domain baru dan memigrasi data Anda. Begitu juga sebaliknya. Jika Anda membuat domain dalam VPC, domain tersebut tidak dapat memiliki titik akhir publik. Sebagai gantinya, Anda harus membuat domain lain atau menonaktifkan kontrol ini.

Lihat Meluncurkan domain OpenSearch Layanan Amazon Anda dalam VPC di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/4.2.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-node-to-node-encryption-check`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan enkripsi node-ke-node. Kontrol gagal jika domain Elasticsearch tidak mengaktifkan enkripsi node-ke-node. Kontrol juga

menghasilkan temuan yang gagal jika versi Elasticsearch tidak mendukung pemeriksaan enkripsi node-ke-node.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan serangan person-in-the-middle atau serupa. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang boleh diizinkan. Mengaktifkan enkripsi node-ke-node untuk domain Elasticsearch memastikan bahwa komunikasi intra-cluster dienkripsi saat transit.

Mungkin ada penalti kinerja yang terkait dengan konfigurasi ini. Anda harus mengetahui dan menguji pertukaran kinerja sebelum mengaktifkan opsi ini.

Remediasi

Untuk informasi tentang mengaktifkan enkripsi node-ke-node pada domain baru dan yang sudah ada, lihat Meng aktifkan enkripsi node-ke-node di Panduan Pengembang Layanan Amazon. OpenSearch

[ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi - Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-logs-to-cloudwatch`

Jenis jadwal: Perubahan dipicu

Parameter:

- `logtype = 'error'`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi untuk mengirim log kesalahan ke CloudWatch Log.

Anda harus mengaktifkan log kesalahan untuk domain Elasticsearch dan mengirim log tersebut ke CloudWatch Log untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk informasi tentang cara mengaktifkan penerbitan log, lihat Meng aktifkan penerbitan log (konsol) di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.5] Domain Elasticsearch harus mengaktifkan logging audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-audit-logging-enabled` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

- `cloudWatchLogsLogGroupArnList`(tidak dapat disesuaikan). Security Hub CSPM tidak mengisi parameter ini. Comma-separated daftar grup CloudWatch log log yang harus dikonfigurasi untuk log audit.

  Aturan ini adalah `NON_COMPLIANT` jika grup CloudWatch log log dari domain Elasticsearch tidak ditentukan dalam daftar parameter ini.

Kontrol ini memeriksa apakah domain Elasticsearch mengaktifkan logging audit. Kontrol ini gagal jika domain Elasticsearch tidak mengaktifkan logging audit.

Log audit sangat dapat disesuaikan. Mereka memungkinkan Anda untuk melacak aktivitas pengguna di cluster Elasticsearch Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan ke OpenSearch, perubahan indeks, dan permintaan pencarian yang masuk.

Remediasi

Untuk petunjuk terperinci tentang mengaktifkan log audit, lihat Mengaktifkan log audit di Panduan Pengembang OpenSearch Layanan Amazon.

[ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-data-node-fault-tolerance` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi dengan setidaknya tiga node data dan `zoneAwarenessEnabled` is`true`.

Domain Elasticsearch membutuhkan setidaknya tiga node data untuk ketersediaan tinggi dan toleransi kesalahan. Menyebarkan domain Elasticsearch dengan setidaknya tiga node data memastikan operasi cluster jika node gagal.

Remediasi

Untuk mengubah jumlah node data dalam domain Elasticsearch

1. Buka konsol OpenSearch Layanan Amazon di https://console.aws.amazon.com/aos/.
2. Di bawah Domain, pilih nama domain yang ingin Anda edit.
3. Pilih Edit domain.
4. Di bawah Data node, atur Jumlah node ke angka yang lebih besar dari atau sama dengan`3`.

   Untuk tiga penerapan Zona Ketersediaan, setel ke kelipatan tiga untuk memastikan distribusi yang sama di seluruh Zona Ketersediaan.

5. Pilih Kirim.

[ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-primary-node-fault-tolerance` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain Elasticsearch dikonfigurasi dengan setidaknya tiga node utama khusus. Kontrol ini gagal jika domain tidak menggunakan node primer khusus. Kontrol ini lolos jika domain Elasticsearch memiliki lima node utama khusus. Namun, menggunakan lebih dari tiga node utama mungkin tidak diperlukan untuk mengurangi risiko ketersediaan, dan akan mengakibatkan biaya tambahan.

Domain Elasticsearch membutuhkan setidaknya tiga node utama khusus untuk ketersediaan tinggi dan toleransi kesalahan. Sumber daya node primer khusus dapat tegang selama penerapan node blue/green data karena ada node tambahan untuk dikelola. Menyebarkan domain Elasticsearch dengan setidaknya tiga node primer khusus memastikan kapasitas sumber daya node primer yang memadai dan operasi cluster jika node gagal.

Remediasi

Untuk memodifikasi jumlah node primer khusus dalam OpenSearch domain

1. Buka konsol OpenSearch Layanan Amazon di https://console.aws.amazon.com/aos/.
2. Di bawah Domain, pilih nama domain yang ingin Anda edit.
3. Pilih Edit domain.
4. Di bawah Node master khusus, set el tipe Inst ance ke jenis instance yang diinginkan.

5. A tur Jumlah node master sama dengan tiga atau lebih besar.
6. Pilih Kirim.

[ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

Persyaratan terkait: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6), PCI DSS v4.0. 1/4.2.1

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `elasticsearch-https-required` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akhir domain Elasticsearch dikonfigurasi untuk menggunakan kebijakan keamanan TLS terbaru. Kontrol gagal jika titik akhir domain Elasticsearch tidak dikonfigurasi untuk menggunakan kebijakan terbaru yang didukung atau jika HTTPS tidak diaktifkan. Kebijakan keamanan TLS terbaru yang didukung saat ini adalah`Policy-Min-TLS-1-2-PFS-2023-10`.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan serangan person-in-the-middle atau serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang boleh diizinkan. Mengenkripsi data dalam transit dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS. TLS 1.2 menyediakan beberapa peningkatan keamanan dibandingkan versi TLS sebelumnya.

Remediasi

Untuk mengaktifkan enkripsi TLS, gunakan operasi UpdateDomainConfig API untuk mengkonfigurasi DomainEndpointOptions objek. Ini mengatur`TLSSecurityPolicy`.

[ES.9] Domain Elasticsearch harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Elasticsearch::Domain`

AWS Config aturan: `tagged-elasticsearch-domain` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	`No default value`

Kontrol ini memeriksa apakah domain Elasticsearch memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika domain tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika domain tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke domain Elasticsearch, lihat Bek erja dengan tag di Panduan Pengembang OpenSearch Layanan Amazon.

Kontrol CSPM Security Hub untuk Amazon EMR

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon EMR (sebelumnya disebut Amazon Elastic MapReduce). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::EMR::Cluster`

AWS Configaturan: emr-master-no-public-ip

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah node master di klaster EMR Amazon memiliki alamat IP publik. Kontrol gagal jika alamat IP publik dikaitkan dengan salah satu instance node master.

Alamat IP publik ditunjuk di `PublicIp` bidang `NetworkInterfaces` konfigurasi untuk instance. Kontrol ini hanya memeriksa kluster EMR Amazon yang berada dalam status atau`RUNNING`. `WAITING`

Remediasi

Selama peluncuran, Anda dapat mengontrol apakah instance Anda di subnet default atau nondefault diberi alamat IPv4 publik. Secara default, subnet default memiliki atribut ini disetel k`true`. Subnet nondefault memiliki atribut pengalamatan publik IPv4 yang disetel k`false`, kecuali jika dibuat oleh wizard instans peluncuran Amazon EC2. Dalam hal ini, atribut diatur k`true`.

Setelah diluncurkan, Anda tidak dapat secara manual memisahkan alamat IPv4 publik dari instans Anda.

Untuk memulihkan temuan yang gagal, Anda harus meluncurkan cluster baru di VPC dengan subnet pribadi yang memiliki atribut pengalamatan publik IPv4 yang disetel ke. `false` Untuk petunjuknya, lihat Meluncurkan cluster ke dalam VPC di Panduan Manajemen EMR Amazon.

[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/1.4.4, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: emr-block-public-access

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akun Anda dikonfigurasi dengan Amazon EMR memblokir akses publik. Kontrol gagal jika pengaturan blokir akses publik tidak diaktifkan atau jika port apa pun selain port 22 diizinkan.

Amazon EMR memblokir akses publik mencegah Anda meluncurkan cluster di subnet publik jika cluster memiliki konfigurasi keamanan yang memungkinkan lalu lintas masuk dari alamat IP publik pada port. Saat pengguna dari Anda Akun AWS meluncurkan kluster, Amazon EMR memeriksa aturan port di grup keamanan untuk klaster dan membandingkannya dengan aturan lalu lintas masuk Anda. Jika grup keamanan memiliki aturan masuk yang membuka port ke alamat IP publik IPv4 0.0.0.0/0 atau IPv6: :/0, dan port tersebut tidak ditentukan sebagai pengecualian untuk akun Anda, Amazon EMR tidak mengizinkan pengguna membuat cluster.

> **Note**
>
> Blokir akses publik diaktifkan secara default. Untuk meningkatkan perlindungan akun, kami sarankan Anda tetap mengaktifkannya.

Remediasi

Untuk mengonfigurasi blokir akses publik untuk Amazon EMR, lihat Menggunakan Amazon EMR memblokir akses publik di Panduan Manajemen EMR Amazon.

[EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EMR::SecurityConfiguration`

AWS Configaturan: emr-security-configuration-encryption-rest

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konfigurasi keamanan EMR Amazon mengaktifkan enkripsi saat istirahat. Kontrol gagal jika konfigurasi keamanan tidak mengaktifkan enkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat dalam konfigurasi keamanan Amazon EMR, lihat Mengonfigurasi enkripsi data di Panduan Manajemen EMR Amazon.

[EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-7 (4) NIST.800-53.r5 SC-8,, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::EMR::SecurityConfiguration`

AWS Configaturan: emr-security-configuration-encryption-transit

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konfigurasi keamanan EMR Amazon mengaktifkan enkripsi saat transit. Kontrol gagal jika konfigurasi keamanan tidak mengaktifkan enkripsi dalam perjalanan.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara cluster Anda dan aplikasi Anda. Data dapat bergerak di internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Untuk mengaktifkan enkripsi saat transit dalam konfigurasi keamanan Amazon EMR, lihat Mengonfigurasi enkripsi data di Panduan Manajemen EMR Amazon.

Kontrol CSPM Security Hub untuk EventBridge

AWS Security Hub CSPMKontrol ini mengevaluasi EventBridge layanan dan sumber daya Amazon.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[EventBridge.2] bus EventBridge acara harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Events::EventBus`

AWS Configaturan: `tagged-events-eventbus` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah bus EventBridge acara Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika bus acara tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika bus acara tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan,

pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke bus EventBridge acara, lihat EventBridge Tag Amazon di Panduan EventBridge Pengguna Amazon.

[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3), PCI DSS v4.0. 1/10.3.1

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Events::EventBus`

AWS Configaturan: custom-eventbus-policy-attached

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bus acara EventBridge khusus Amazon memiliki kebijakan berbasis sumber daya yang dilampirkan. Kontrol ini gagal jika bus acara khusus tidak memiliki kebijakan berbasis sumber daya.

Secara default, bus acara EventBridge khusus tidak memiliki kebijakan berbasis sumber daya yang dilampirkan. Hal ini memungkinkan kepala sekolah di akun untuk mengakses bus acara. Dengan melampirkan kebijakan berbasis sumber daya ke bus acara, Anda dapat membatasi akses ke bus acara ke akun tertentu, serta dengan sengaja memberikan akses ke entitas di akun lain.

Remediasi

Untuk melampirkan kebijakan berbasis sumber daya ke bus peristiwa EventBridge khusus, lihat Menggunakan kebijakan berbasis sumber daya untuk Amazon di Panduan Pengguna Amazon. EventBridge EventBridge

[EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Events::Endpoint`

AWS Configaturan: **`global-endpoint-event-replication-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah replikasi peristiwa diaktifkan untuk titik akhir EventBridge global Amazon. Kontrol gagal jika replikasi peristiwa tidak diaktifkan untuk titik akhir global.

Titik akhir global membantu membuat aplikasi Anda Regional-fault toleran. Untuk memulai, Anda menetapkan pemeriksaan kesehatan Amazon Route 53 ke titik akhir. Ketika failover dimulai, pemeriksaan kesehatan melaporkan keadaan “tidak sehat”. Dalam beberapa menit setelah inisiasi failover, semua acara khusus diarahkan ke bus acara di Wilayah sekunder dan diproses oleh bus acara tersebut. Saat Anda menggunakan titik akhir global, Anda dapat mengaktifkan replikasi peristiwa. Replikasi acara mengirimkan semua peristiwa khusus ke bus acara di Wilayah primer dan

sekunder menggunakan aturan terkelola. Sebaiknya aktifkan replikasi peristiwa saat menyiapkan titik akhir global. Replikasi acara membantu Anda memverifikasi bahwa titik akhir global Anda dikonfigurasi dengan benar. Replikasi peristiwa diperlukan untuk memulihkan secara otomatis dari peristiwa failover. Jika replikasi acara tidak diaktifkan, Anda harus mengatur ulang pemeriksaan kesehatan Route 53 secara manual ke “sehat” sebelum acara dialihkan kembali ke Wilayah utama.

> **Note**
>
> Jika Anda menggunakan bus acara khusus, Anda memerlukan bus genap khusus di setiap Wilayah dengan nama yang sama dan di akun yang sama agar failover berfungsi dengan baik. Mengaktifkan replikasi acara dapat meningkatkan biaya bulanan Anda. Untuk informasi tentang harga, lihat EventBridge harga Amazon.

Remediasi

Untuk mengaktifkan replikasi peristiwa untuk titik akhir EventBridge global, lihat Membuat titik akhir global di Panduan Pengguna Amazon EventBridge . Untuk replikasi Acara, pilih Replikasi acara diaktifkan.

Kontrol CSPM Security Hub untuk Amazon Fraud Detector

Kontrol CSPM Security Hub ini mengevaluasi layanan dan sumber daya Amazon Fraud Detector.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::EntityType`

AWS Configaturan: `frauddetector-entity-type-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah jenis entitas Amazon Fraud Detector memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika tipe entitas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tipe entitas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke jenis entitas Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di https://console.aws.amazon.com/frauddetector.
2. Di panel navigasi, pilih Entitas.
3. Pilih jenis entitas dari daftar.
4. Di bagian tag tipe entitas, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[FraudDetector.2] Label Amazon Fraud Detector harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::Label`

AWS Configaturan: `frauddetector-label-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah label Amazon Fraud Detector memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika label tidak memiliki kunci tag atau

jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika label tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke label Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di https://console.aws.amazon.com/frauddetector.
2. Di panel navigasi, pilih Label.
3. Pilih label dari daftar.
4. Di bagian tag label, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::Outcome`

AWS Configaturan: `frauddetector-outcome-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah hasil Amazon Fraud Detector memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika hasilnya tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika hasilnya tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM

(pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke hasil Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di https://console.aws.amazon.com/frauddetector.
2. Di panel navigasi, pilih Hasil.
3. Pilih hasil dari daftar.
4. Di bagian tag hasil, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

[FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FraudDetector::Variable`

AWS Configaturan: `frauddetector-variable-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah variabel Amazon Fraud Detector memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika variabel tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika variabel tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke variabel Amazon Fraud Detector (konsol)

1. Buka konsol Amazon Fraud Detector di https://console.aws.amazon.com/frauddetector.
2. Di panel navigasi, pilih Variabel.
3. Pilih variabel dari daftar.
4. Di bagian tag variabel, pilih Kelola tag.
5. Pilih Tambahkan tag baru. Masukkan kunci dan nilai untuk tanda tersebut. Ulangi untuk pasangan nilai kunci tambahan.
6. Setelah Anda selesai menambahkan tanda, pilih Simpan.

Kontrol CSPM Security Hub untuk Amazon FSx

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon FSx. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FSx::FileSystem`

AWS Configaturan: fsx-openzfs-copy-tags-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk OpenZFS dikonfigurasi untuk menyalin tag ke cadangan dan volume. Kontrol gagal jika sistem file OpenZFS tidak dikonfigurasi untuk menyalin tag ke backup dan volume.

Identifikasi dan inventaris aset TI Anda merupakan aspek penting dari tata kelola dan keamanan. Tag membantu Anda mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya,

berdasarkan tujuan, pemilik, atau lingkungan. Ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama karena Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang Anda tetapkan padanya.

Remediasi

Untuk informasi tentang mengonfigurasi sistem file FSx untuk OpenZFS untuk menyalin tag ke cadangan dan volume, lihat Memperbarui sistem file di Amazon FSx untuk Panduan Pengguna OpenZFS.

[FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan

Persyaratan terkait: NIST.800-53.r5 CP-9, NIST.800-53.r5 CM-8

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::FSx::FileSystem`

AWS Configaturan: fsx-lustre-copy-tags-to-backups

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sistem file Amazon FSx for Lustre dikonfigurasi untuk menyalin tag ke backup dan volume. Kontrol gagal jika sistem file Lustre tidak dikonfigurasi untuk menyalin tag ke backup dan volume.

Identifikasi dan inventaris aset TI Anda merupakan aspek penting dari tata kelola dan keamanan. Tag membantu Anda mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama karena Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang Anda tetapkan padanya.

Remediasi

Untuk informasi tentang mengonfigurasi sistem file FSx for Lustre untuk menyalin tag ke cadangan, lihat Menyalin cadangan dalam hal yang sama Akun AWS di Panduan Pengguna Amazon FSx for Lustre.

[FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::FSx::FileSystem`

AWS Configaturan: fsx-openzfs-deployment-type-check

Jenis jadwal: Periodik

Parameter: `deploymentTypes: MULTI_AZ_1` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk OpenZFS dikonfigurasi untuk menggunakan beberapa jenis penyebaran Availability Zones ()Multi-AZ. Kontrol gagal jika sistem file tidak dikonfigurasi untuk menggunakan jenis Multi-AZ penerapan.

Amazon FSx untuk OpenZFS mendukung beberapa jenis penyebaran untuk sistem file: Multi-AZ (HA), (HA), dan Single-AZ (non-HA). Single-AZ Jenis penyebaran menawarkan tingkat ketersediaan dan daya tahan yang berbeda. Multi-AZ Sistem file (HA) terdiri dari sepasang server file ketersediaan tinggi (HA) yang tersebar di dua Availability Zones (AZ). Kami merekomendasikan penggunaan tipe penerapan Multi-AZ (HA) untuk sebagian besar beban kerja produksi karena ketersediaan tinggi dan model daya tahan yang disediakannya.

Remediasi

Anda dapat mengonfigurasi sistem file Amazon FSx untuk OpenZFS untuk menggunakan jenis Multi-AZ penyebaran saat Anda membuat sistem file. Anda tidak dapat mengubah jenis penerapan untuk sistem file FSx untuk OpenZFS yang ada.

Untuk informasi tentang jenis dan opsi penerapan FSx untuk sistem file OpenZFS, lihat Ketersediaan dan daya tahan Amazon FSx untuk OpenZFS dan Mengelola sumber daya sistem file di Amazon FSx untuk Panduan Pengguna OpenZFS.

[FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::FSx::FileSystem`

AWS Configaturan: fsx-ontap-deployment-type-check

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`deploymentTypes`	Daftar jenis penyebaran untuk disertakan dalam evaluasi. Kontrol menghasilkan `FAILED` temuan jika sistem file tidak dikonfigurasi untuk menggunakan jenis penerapan yang ditentukan dalam daftar.	Enum	`MULTI_AZ_1` , `MULTI_AZ_2`	`MULTI_AZ_1` , `MULTI_AZ_2`

Kontrol ini memeriksa apakah sistem file Amazon FSx untuk NetApp ONTAP dikonfigurasi untuk menggunakan beberapa jenis penyebaran Availability Zones (Multi-AZ). Kontrol gagal jika sistem file tidak dikonfigurasi untuk menggunakan jenis Multi-AZ penerapan. Anda dapat secara opsional menentukan daftar jenis penerapan yang akan disertakan dalam evaluasi.

Amazon FSx untuk NetApp ONTAP mendukung beberapa jenis penyebaran untuk sistem file: Single-AZ 1, Single-AZ 2, 1, dan 2. Multi-AZ Multi-AZ Jenis penyebaran menawarkan tingkat ketersediaan dan daya tahan yang berbeda. Sebaiknya gunakan jenis Multi-AZ penerapan untuk sebagian besar beban kerja produksi karena model ketersediaan dan daya tahan tinggi yang disediakan oleh tipe Multi-AZ penerapan. Multi-AZ sistem file mendukung semua fitur ketersediaan dan daya tahan sistem Single-AZ file. Selain itu, mereka dirancang untuk menyediakan ketersediaan berkelanjutan ke data bahkan ketika Availability Zone (AZ) tidak tersedia.

Remediasi

Anda tidak dapat mengubah jenis penerapan untuk sistem file Amazon FSx NetApp untuk ONTAP yang ada. Namun, Anda dapat mencadangkan data, dan kemudian mengembalikannya pada sistem file baru yang menggunakan jenis Multi-AZ penyebaran.

Untuk informasi tentang jenis dan opsi penerapan FSx untuk sistem file ONTAP, lihat Opsi ketersediaan, daya tahan, dan penerapan serta Mengelola sistem file di FSx untuk Panduan Pengguna ONTAP.

[FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::FSx::FileSystem`

AWS Configaturan: fsx-windows-deployment-type-check

Jenis jadwal: Periodik

Parameter: `deploymentTypes: MULTI_AZ_1` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah sistem file Amazon FSx for Windows File Server dikonfigurasi untuk menggunakan beberapa jenis penyebaran Availability Zones Multi-AZ (). Kontrol gagal jika sistem file tidak dikonfigurasi untuk menggunakan jenis Multi-AZ penerapan.

Amazon FSx for Windows File Server mendukung dua jenis penyebaran untuk sistem Single-AZfile: dan. Multi-AZ Jenis penyebaran menawarkan tingkat ketersediaan dan daya tahan yang berbeda. Single-AZ Sistem file terdiri dari satu instance server file Windows dan satu set volume penyimpanan dalam satu Availability Zone (AZ). Multi-AZ Sistem file terdiri dari cluster ketersediaan tinggi server file Windows yang tersebar di dua Availability Zone. Kami merekomendasikan penggunaan jenis Multi-AZ penyebaran untuk sebagian besar beban kerja produksi karena ketersediaan tinggi dan model daya tahan yang disediakannya.

Remediasi

Anda dapat mengonfigurasi sistem file Amazon FSx for Windows File Server untuk menggunakan Multi-AZ jenis penyebaran saat Anda membuat sistem file. Anda tidak dapat mengubah jenis penerapan untuk sistem file FSx for Windows File Server yang ada.

Untuk informasi tentang jenis dan opsi penerapan untuk sistem file FSx for Windows File Server, lihat Ketersediaan dan daya tahan Single-AZ : dan sistem file Multi-AZ dan Memulai dengan Amazon FSx for Windows File Server di Panduan Pengguna Amazon FSx for Windows File Server.

Kontrol CSPM Security Hub untuk Global Accelerator

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Global Accelerator layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GlobalAccelerator::Accelerator`

AWS Configaturan: `tagged-globalaccelerator-accelerator` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah AWS Global Accelerator akselerator memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika akselerator tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika akselerator tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke akselerator global Akselerator Global, lihat Menandai AWS Global Accelerator di Panduan PengembangAWS Global Accelerator.

Kontrol CSPM Security Hub untukAWS Glue

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Glue layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Glue.1]AWS Gluepekerjaan harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Glue::Job`

AWS Configaturan: `tagged-glue-job` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Glue pekerjaan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika pekerjaan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pekerjaan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS Glue pekerjaan, lihat AWStag AWS Glue di Panduan AWS Glue Pengguna.

[Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Glue::MLTransform`

AWS Configaturan: glue-ml-transform-encrypted-at-rest

Jenis jadwal: Perubahan dipicu

Parameter: Tidak

Kontrol ini memeriksa apakah transformasi pembelajaran AWS Glue mesin dienkripsi saat istirahat. Kontrol gagal jika transformasi pembelajaran mesin tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengonfigurasi enkripsi untuk transformasi pembelajaran AWS Glue mesin, lihat Bekerja dengan transformasi pembelajaran mesin di AWS GluePanduan Pengguna.

[Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2,, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Glue::Job`

AWS Configaturan: glue-spark-job-supported-version

Jenis jadwal: Perubahan dipicu

Parameter:`minimumSupportedGlueVersion`: `3.0` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pekerjaan AWS Glue for Spark dikonfigurasi untuk berjalan pada versi yang didukung. AWS Glue Kontrol gagal jika pekerjaan Spark dikonfigurasi untuk berjalan pada versi yang lebih awal dari versi minimum yang didukung. AWS Glue

> **Note**
>
> Kontrol ini juga menghasilkan `FAILED` temuan untuk pekerjaan Spark jika properti AWS Glue version (`GlueVersion`) tidak ada atau null dalam item konfigurasi (CI) untuk pekerjaan tersebut. AWS Glue Dalam kasus seperti itu, temuan tersebut mencakup anotasi berikut:`GlueVersion is null or missing in glueetl job configuration`. Untuk mengatasi jenis `FAILED` temuan ini, tambahkan `GlueVersion` properti ke konfigurasi pekerjaan. Untuk daftar versi dan lingkungan runtime yang didukung, lihat AWS GlueVersi dalam Panduan AWS Glue Pengguna.

Menjalankan pekerjaan AWS Glue Spark pada versi saat ini AWS Glue dapat mengoptimalkan kinerja, keamanan, dan akses ke fitur terbaru. AWS Glue Ini juga dapat membantu melindungi terhadap kerentanan keamanan. Misalnya, versi baru mungkin dirilis untuk menyediakan pembaruan keamanan, mengatasi masalah, atau memperkenalkan fitur baru.

Remediasi

Untuk informasi tentang memigrasi pekerjaan Spark ke versi yang didukungAWS Glue, lihat Memigrasi AWS Glue pekerjaan Spark di Panduan Pengguna. AWS Glue

Kontrol CSPM Security Hub untuk Amazon GuardDuty

AWS Security Hub CSPMKontrol ini mengevaluasi GuardDuty layanan dan sumber daya Amazon. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[GuardDuty.1] GuardDuty harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5) NIST.800-53.r5 CA-7,, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 RA-3 (4), NIST.800-53.r5 SA-11 (1), NIST.800-53.r5 SA-11 (6), NIST.800-53.r5 SA-15 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SA-8 (21), NIST.800-53.r5 SA-8 (25) NIST.800-53.r5 SC-5,, NIST.800-53.r5 SC-5 (1), NIST.800-53.r5 SC-5 (3) NIST.800-53.r5 SI-20,, NIST.800-53.r5 SI-3 (8) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4(1), NIST.800-53.r5 SI-4 (13), NIST.800-53.r5 SI-4 (2), (22), NIST.800-53.r5 SI-4 (25), NIST.800-53.r5 SI-4 (4), NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-4 (5), NIST.800-171.r2 3.4.2, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2. 1/11.4, PCI DSS v4.0. 1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: guardduty-enabled-centralized

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Amazon GuardDuty diaktifkan di GuardDuty akun dan Wilayah Anda.

Sangat disarankan agar Anda mengaktifkan GuardDuty di semua AWS Wilayah yang didukung. Melakukannya memungkinkan GuardDuty untuk menghasilkan temuan tentang aktivitas yang tidak sah atau tidak biasa, bahkan di Wilayah yang tidak Anda gunakan secara aktif. Ini juga memungkinkan GuardDuty untuk memantau CloudTrail peristiwa untuk global Layanan AWS seperti IAM.

Remediasi

Untuk mengaktifkan GuardDuty, lihat Memulai GuardDuty di Panduan GuardDuty Pengguna Amazon.

[GuardDuty.2] GuardDuty filter harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GuardDuty::Filter`

AWS Configaturan: `tagged-guardduty-filter` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah GuardDuty filter Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika filter tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika filter tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke GuardDuty filter, lihat TagResourcedi Referensi Amazon GuardDuty API.

[GuardDuty.3] GuardDuty IPset harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GuardDuty::IPSet`

AWS Configaturan: `tagged-guardduty-ipset` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah Amazon GuardDuty IPSet memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika IPSet tidak memiliki kunci tag

atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika IPSet tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke GuardDuty IPSet, lihat TagResourcedi Referensi Amazon GuardDuty API.

[GuardDuty.4] GuardDuty detektor harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: `tagged-guardduty-detector` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah GuardDuty detektor Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika detektor tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika detektor tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke GuardDuty detektor, lihat TagResourcedi Referensi Amazon GuardDuty API.

[GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-eks-protection-audit-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Pemantauan Log Audit GuardDuty EKS diaktifkan. Untuk akun mandiri, kontrol gagal jika Pemantauan Log Audit GuardDuty EKS dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Pemantauan Log Audit EKS.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Pemantauan Log Audit EKS untuk akun anggota di organisasi. GuardDuty akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Pemantauan Log Audit GuardDuty EKS. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

GuardDuty Pemantauan Log Audit EKS membantu Anda mendeteksi aktivitas yang berpotensi mencurigakan di kluster Amazon Elastic Kubernetes Service (Amazon EKS). EKS Audit Log Monitoring menggunakan log audit Kubernetes untuk menangkap aktivitas kronologis dari pengguna, aplikasi yang menggunakan Kubernetes API, dan control plane.

Remediasi

Untuk mengaktifkan Pemantauan Log Audit GuardDuty EKS, lihat Pemantauan Log Audit EKS di Panduan GuardDuty Pengguna Amazon.

[GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-lambda-protection-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty Lambda diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty Lambda dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan Lambda.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan Lambda untuk akun anggota di organisasi. GuardDuty akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty Lambda. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

GuardDuty Perlindungan Lambda membantu Anda mengidentifikasi potensi ancaman keamanan saat suatu AWS Lambda fungsi dipanggil. Setelah Anda mengaktifkan Perlindungan Lambda, GuardDuty mulai memantau log aktivitas jaringan Lambda yang terkait dengan fungsi Lambda di Anda. Akun AWS Ketika fungsi Lambda dipanggil dan GuardDuty mengidentifikasi lalu lintas jaringan mencurigakan yang menunjukkan adanya potongan kode yang berpotensi berbahaya dalam fungsi Lambda Anda, menghasilkan temuan. GuardDuty

Remediasi

Untuk mengaktifkan Perlindungan GuardDuty Lambda, lihat Mengonfigurasi Perlindungan Lambda di Panduan Pengguna Amazon. GuardDuty

[GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/11.5.1

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-eks-protection-runtime-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah GuardDuty EKS Runtime Monitoring dengan manajemen agen otomatis diaktifkan. Untuk akun mandiri, kontrol gagal jika GuardDuty EKS Runtime Monitoring dengan manajemen agen otomatis dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak memiliki EKS Runtime Monitoring dengan manajemen agen otomatis diaktifkan.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur EKS Runtime Monitoring dengan manajemen agen otomatis untuk akun anggota di organisasi. GuardDuty akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan GuardDuty EKS Runtime Monitoring. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

Perlindungan EKS di Amazon GuardDuty menyediakan cakupan deteksi ancaman untuk membantu Anda melindungi kluster Amazon EKS di AWS lingkungan Anda. EKS Runtime Monitoring menggunakan peristiwa tingkat sistem operasi untuk membantu Anda mendeteksi potensi ancaman di node dan kontainer EKS dalam kluster EKS Anda.

Remediasi

Untuk mengaktifkan Pemantauan Runtime EKS dengan manajemen agen otomatis, lihat Mengaktifkan Pemantauan GuardDuty Runtime di Panduan Pengguna Amazon GuardDuty .

[GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-malware-protection-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty Malware diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty Malware dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan Malware.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan Malware untuk akun anggota di organisasi. GuardDuty akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty Malware. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

GuardDuty Perlindungan Malware untuk EC2 membantu Anda mendeteksi potensi keberadaan malware dengan memindai volume Amazon Elastic Block Store (Amazon EBS) yang dilampirkan ke instans Amazon Elastic Compute Cloud (Amazon EC2) dan beban kerja container. Perlindungan Malware menyediakan opsi pemindaian di mana Anda dapat memutuskan apakah Anda ingin menyertakan atau mengecualikan instans EC2 tertentu dan beban kerja kontainer pada saat pemindaian. Ini juga menyediakan opsi untuk menyimpan snapshot volume EBS yang dilampirkan ke instans EC2 atau beban kerja kontainer, di akun Anda. GuardDuty Cuplikan disimpan hanya ketika malware ditemukan dan temuan Perlindungan Malware dihasilkan.

Remediasi

Untuk mengaktifkan Perlindungan GuardDuty Malware untuk EC2, lihat Mengonfigurasi pemindaian GuardDuty-initiated malware di GuardDuty Panduan Pengguna Amazon.

[GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-rds-protection-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty RDS diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty RDS dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan RDS.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan RDS untuk akun anggota di organisasi. GuardDuty akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty RDS. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

Perlindungan RDS dalam GuardDuty analisis dan profil Aktivitas login RDS untuk potensi ancaman akses ke database Amazon Aurora Anda (Edisi Aurora dan Edisi Aurora MySQL-Compatible). PostgreSQL-Compatible Fitur ini memungkinkan Anda mengidentifikasi perilaku login yang berpotensi mencurigakan. Perlindungan RDS tidak memerlukan infrastruktur tambahan dan dirancang agar tidak memengaruhi kinerja instans basis data Anda. Ketika RDS Protection mendeteksi upaya login yang berpotensi mencurigakan atau anomali yang menunjukkan ancaman terhadap database Anda, GuardDuty menghasilkan temuan baru dengan detail tentang database yang berpotensi dikompromikan.

Remediasi

Untuk mengaktifkan Perlindungan GuardDuty RDS, lihat Perlindungan GuardDuty RDS di GuardDuty Panduan Pengguna Amazon.

[GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/11.5.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-s3-protection-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Perlindungan GuardDuty S3 diaktifkan. Untuk akun mandiri, kontrol gagal jika Perlindungan GuardDuty S3 dinonaktifkan di akun. Dalam lingkungan multi-akun, kontrol gagal jika akun GuardDuty administrator yang didelegasikan dan semua akun anggota tidak mengaktifkan Perlindungan S3.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur Perlindungan S3 untuk akun anggota di organisasi. GuardDuty akun anggota tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika GuardDuty administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan Perlindungan GuardDuty S3. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini. GuardDuty

S3 Protection memungkinkan GuardDuty untuk memantau operasi API tingkat objek untuk mengidentifikasi potensi risiko keamanan data dalam bucket Amazon Simple Storage Service (Amazon S3). GuardDuty memantau ancaman terhadap sumber daya S3 Anda dengan menganalisis peristiwa AWS CloudTrail manajemen dan peristiwa data CloudTrail S3.

Remediasi

Untuk mengaktifkan Perlindungan GuardDuty S3, lihat Perlindungan Amazon S3 di GuardDuty Amazon di Panduan Pengguna GuardDuty Amazon.

[GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-runtime-monitoring-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Runtime Monitoring diaktifkan di Amazon GuardDuty. Untuk akun mandiri, kontrol gagal jika GuardDuty Runtime Monitoring dinonaktifkan untuk akun tersebut. Dalam lingkungan multi-akun, kontrol gagal jika GuardDuty Runtime Monitoring dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan dan semua akun anggota.

Dalam lingkungan multi-akun, hanya GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan GuardDuty Runtime Monitoring untuk akun di organisasi mereka. Selain itu, hanya GuardDuty administrator yang dapat mengonfigurasi dan mengelola agen keamanan yang GuardDuty digunakan untuk pemantauan runtime AWS beban kerja dan sumber daya untuk akun di organisasi. GuardDuty akun anggota tidak dapat mengaktifkan, mengonfigurasi, atau menonaktifkan Runtime Monitoring untuk akun mereka sendiri.

GuardDuty Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda. Ini menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Anda dapat mengaktifkan dan mengelola agen keamanan untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman, seperti kluster Amazon EKS dan instans Amazon EC2.

Remediasi

Untuk informasi tentang mengonfigurasi dan mengaktifkan GuardDuty Runtime Monitoring, lihat Runtime Monitoring dan Mengaktifkan GuardDuty Runtime Monitoring di GuardDuty Panduan Pengguna Amazon. GuardDuty

[GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-ecs-protection-runtime-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah agen keamanan GuardDuty otomatis Amazon diaktifkan untuk pemantauan runtime kluster Amazon ECS aktif. AWS Fargate Untuk akun mandiri, kontrol gagal jika agen keamanan dinonaktifkan untuk akun tersebut. Dalam lingkungan multi-akun, kontrol gagal jika agen keamanan dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan dan semua akun anggota.

Dalam lingkungan multi-akun, kontrol ini menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Ini karena hanya GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Runtime Monitoring sumber ECS-Fargate daya untuk akun di organisasi mereka. GuardDuty Akun anggota tidak dapat melakukan ini untuk akun mereka sendiri. Selain itu, kontrol ini menghasilkan `FAILED` temuan jika GuardDuty ditangguhkan untuk akun anggota dan Pemantauan Runtime sumber ECS-Fargate daya dinonaktifkan untuk akun anggota. Untuk menerima `PASSED` temuan, GuardDuty administrator harus memisahkan akun anggota yang ditangguhkan dari akun administrator mereka dengan menggunakan GuardDuty.

GuardDuty Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda. Ini menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Anda dapat mengaktifkan dan mengelola agen keamanan untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman. Ini termasuk kluster Amazon ECS di. AWS Fargate

Remediasi

Untuk mengaktifkan dan mengelola agen keamanan untuk GuardDuty Runtime Monitoring sumber ECS-Fargate daya, Anda harus menggunakannya GuardDuty secara langsung. Anda tidak dapat mengaktifkan atau mengelolanya secara manual untuk ECS-Fargate sumber daya. Untuk informasi tentang mengaktifkan dan mengelola agen keamanan, lihat Prasyarat untuk dukungan AWS Fargate (khusus Amazon ECS) dan Mengelola agen keamanan otomatis untuk AWS Fargate (khusus Amazon ECS) di Panduan Pengguna Amazon. GuardDuty

[GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan

Kategori: Deteksi > Layanan Deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::GuardDuty::Detector`

AWS Configaturan: guardduty-ec2-protection-runtime-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah agen keamanan GuardDuty otomatis Amazon diaktifkan untuk pemantauan runtime instans Amazon EC2. Untuk akun mandiri, kontrol gagal jika agen keamanan dinonaktifkan untuk akun tersebut. Dalam lingkungan multi-akun, kontrol gagal jika agen keamanan dinonaktifkan untuk akun GuardDuty administrator yang didelegasikan dan semua akun anggota.

Dalam lingkungan multi-akun, kontrol ini menghasilkan temuan hanya di akun GuardDuty administrator yang didelegasikan. Ini karena hanya GuardDuty administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan Pemantauan Waktu Proses instans Amazon EC2 untuk akun di organisasi mereka. GuardDuty Akun anggota tidak dapat melakukan ini untuk akun mereka sendiri. Selain itu, kontrol ini menghasilkan `FAILED` temuan jika GuardDuty ditangguhkan untuk akun anggota dan Pemantauan Runtime instans EC2 dinonaktifkan untuk akun anggota. Untuk menerima `PASSED` temuan, GuardDuty administrator harus memisahkan akun anggota yang ditangguhkan dari akun administrator mereka dengan menggunakan GuardDuty.

GuardDuty Runtime Monitoring mengamati dan menganalisis tingkat sistem operasi, jaringan, dan peristiwa file untuk membantu Anda mendeteksi potensi ancaman dalam beban kerja tertentu AWS di lingkungan Anda. Ini menggunakan agen GuardDuty keamanan yang menambahkan visibilitas ke dalam perilaku runtime, seperti akses file, eksekusi proses, argumen baris perintah, dan koneksi jaringan. Anda dapat mengaktifkan dan mengelola agen keamanan untuk setiap jenis sumber daya yang ingin Anda pantau untuk potensi ancaman. Ini termasuk instans Amazon EC2.

Remediasi

Untuk informasi tentang mengonfigurasi dan mengelola agen keamanan otomatis untuk Pemantauan GuardDuty Waktu Proses instans EC2, lihat Prasyarat untuk dukungan instans Amazon EC2 dan Mengaktifkan agen keamanan otomatis untuk instans Amazon EC2 di Panduan Pengguna Amazon. GuardDuty

Kontrol CSPM Security Hub untukAWS Identity and Access Management

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya AWS Identity and Access Management (IAM). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.22, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.16, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6 (10) NIST.800-53.r5 AC-6, (2), NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.4, PCI DSS v3.2. 1/7.2.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::IAM::Policy`

AWS Configaturan: **`iam-policy-no-statements-with-admin-access`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludePermissionBoundaryPolicy: true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah versi default kebijakan IAM (juga dikenal sebagai kebijakan yang dikelola pelanggan) memiliki akses administrator dengan menyertakan pernyataan dengan `"Effect": "Allow"` with `"Action": "*"` over`"Resource": "*"`. Kontrol gagal jika Anda memiliki kebijakan IAM dengan pernyataan seperti itu.

Kontrol hanya memeriksa kebijakan terkelola pelanggan yang Anda buat. Itu tidak memeriksa kebijakan sebaris dan AWS terkelola.

Kebijakan IAM mendefinisikan serangkaian hak istimewa yang diberikan kepada pengguna, grup, atau peran. Mengikuti saran keamanan standar, AWS merekomendasikan agar Anda memberikan hak istimewa paling sedikit, yang berarti hanya memberikan izin yang diperlukan untuk melakukan tugas. Bila Anda memberikan hak administratif penuh alih-alih set izin minimum yang dibutuhkan pengguna, Anda mengekspos sumber daya ke tindakan yang mungkin tidak diinginkan.

Alih-alih mengizinkan hak administratif penuh, tentukan apa yang perlu dilakukan pengguna dan kemudian buat kebijakan yang memungkinkan pengguna hanya melakukan tugas-tugas tersebut. Lebih aman untuk memulai dengan set izin minimum dan memberikan izin tambahan seperlunya. Jangan mulai dengan izin yang terlalu lunak dan kemudian coba kencangkan nanti.

Anda harus menghapus kebijakan IAM yang memiliki pernyataan dengan `"Effect": "Allow"` with `"Action": "*"` over`"Resource": "*"`.

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengubah kebijakan IAM Anda sehingga tidak mengizinkan hak administratif “*” penuh, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.14, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.15, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.16, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1),, (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-53.r5 AC-3 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.1 NIST.800-53.r5 AC-6, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.7, NIST.800-171.r2 3.3.9, 3.13.3, PCI DSS v3.2. NIST.800-171.r2 1/7.2.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: **`iam-user-no-policies-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kebijakan yang dilampirkan. Kontrol gagal jika pengguna IAM Anda memiliki kebijakan yang dilampirkan. Sebagai gantinya, pengguna IAM harus mewarisi izin dari grup IAM atau mengambil peran.

Secara default, pengguna IAM, grup, dan peran tidak memiliki akses ke AWS sumber daya. Kebijakan IAM memberikan hak istimewa kepada pengguna, grup, atau peran. Kami menyarankan Anda menerapkan kebijakan IAM secara langsung ke grup dan peran tetapi tidak untuk pengguna. Menetapkan hak istimewa di grup atau tingkat peran mengurangi kompleksitas manajemen akses seiring bertambahnya jumlah pengguna. Mengurangi kompleksitas manajemen akses pada gilirannya dapat mengurangi kesempatan bagi kepala sekolah untuk secara tidak sengaja menerima atau mempertahankan hak istimewa yang berlebihan.

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengatasi masalah ini, buat grup IAM, dan lampirkan kebijakan ke grup. Kemudian, tambahkan pengguna ke grup. Kebijakan ini diterapkan untuk setiap pengguna dalam grup. Untuk menghapus kebijakan yang dilampirkan langsung ke pengguna, lihat Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna IAM.

[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.13, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.14, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.14, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.4, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.6.3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: **`access-keys-rotated`**

Jenis jadwal: Periodik

Parameter:

- `maxAccessKeyAge`: `90` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kunci akses aktif diputar dalam 90 hari.

Kami sangat menyarankan agar Anda tidak membuat dan menghapus semua kunci akses di akun Anda. Sebaliknya, praktik terbaik yang disarankan adalah membuat satu atau lebih peran IAM atau menggunakan federasi melaluiAWS IAM Identity Center. Anda dapat menggunakan metode ini untuk memungkinkan pengguna Anda mengakses Konsol Manajemen AWS danAWS CLI.

Setiap pendekatan memiliki kasus penggunaannya. Federasi umumnya lebih baik untuk perusahaan yang memiliki direktori pusat yang ada atau berencana untuk membutuhkan lebih dari batas saat ini pada pengguna IAM. Aplikasi yang berjalan di luar AWS lingkungan membutuhkan kunci akses untuk akses terprogram ke AWS sumber daya.

Namun, jika sumber daya yang membutuhkan akses terprogram berjalan di dalamAWS, praktik terbaik adalah menggunakan peran IAM. Peran memungkinkan Anda untuk memberikan akses sumber daya tanpa hardcoding ID kunci akses dan kunci akses rahasia ke dalam konfigurasi.

Untuk mempelajari selengkapnya tentang melindungi kunci akses dan akun Anda, lihat Praktik terbaik untuk mengelola kunci AWS akses di Referensi Umum AWS. Lihat juga panduan posting blog untuk melindungi Anda Akun AWS saat menggunakan akses terprogram.

Jika Anda sudah memiliki kunci akses, Security Hub CSPM merekomendasikan agar Anda memutar kunci akses setiap 90 hari. Memutar kunci akses mengurangi kemungkinan kunci akses yang terkait dengan akun yang disusupi atau dihentikan digunakan. Ini juga memastikan bahwa data tidak dapat diakses dengan kunci lama yang mungkin telah hilang, retak, atau dicuri. Selalu perbarui aplikasi Anda setelah Anda memutar tombol akses.

Kunci akses terdiri dari ID kunci akses dan kunci akses rahasia. Mereka digunakan untuk menandatangani permintaan terprogram yang Anda buat. AWS Pengguna memerlukan kunci akses mereka sendiri untuk melakukan panggilan terprogram AWS dariAWS CLI, Alat untuk Windows PowerShell, AWS SDK, atau panggilan HTTP langsung menggunakan operasi API untuk individu. Layanan AWS

Jika organisasi Anda menggunakan AWS IAM Identity Center (Pusat Identitas IAM), pengguna Anda dapat masuk ke Active Directory, direktori Pusat Identitas IAM bawaan, atau penyedia identitas lain (iDP) yang terhubung ke Pusat Identitas IAM. Mereka kemudian dapat dipetakan ke peran IAM yang memungkinkan mereka menjalankan AWS CLI perintah atau memanggil operasi AWS API tanpa perlu kunci akses. Untuk mempelajari lebih lanjut, lihat Mengonfigurasi AWS CLI yang akan digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna.

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk memutar tombol akses yang lebih tua dari 90 hari, lihat Memutar kunci akses di Panduan Pengguna IAM. Ikuti petunjuk untuk setiap pengguna dengan usia kunci Access lebih dari 90 hari.

[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.3, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.4, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.4, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.12, PCI DSS v3.2. 1/2.1, PCI DSS v3.2. 1/2.2, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-root-access-key-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kunci akses pengguna root ada.

Pengguna root adalah pengguna yang paling istimewa dalam fileAkun AWS. AWSkunci akses menyediakan akses terprogram ke akun tertentu.

Security Hub CSPM merekomendasikan agar Anda menghapus semua kunci akses yang terkait dengan pengguna root. Ini membatasi vektor yang dapat digunakan untuk membahayakan akun Anda. Ini juga mendorong pembuatan dan penggunaan akun berbasis peran yang paling tidak memiliki hak istimewa.

Remediasi

Untuk menghapus kunci akses pengguna root, lihat Menghapus kunci akses untuk pengguna root di Panduan Pengguna IAM. Untuk menghapus kunci akses pengguna root dari Akun AWS dalamAWS GovCloud (US), lihat Menghapus kunci akses pengguna root AWS GovCloud (US) akun saya di Panduan AWS GovCloud (US) Pengguna.

[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.9, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.10, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.10, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), PCI DSS v4.0. 1/8.4.2

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: **`mfa-enabled-for-iam-console-access`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah otentikasi AWS multi-faktor (MFA) diaktifkan untuk semua pengguna IAM yang menggunakan kata sandi konsol.

Multi-factor otentikasi (MFA) menambahkan lapisan perlindungan tambahan di atas nama pengguna dan kata sandi. Dengan MFA diaktifkan, ketika pengguna masuk ke AWS situs web, mereka diminta untuk nama pengguna dan kata sandi mereka. Selain itu, mereka diminta untuk kode otentikasi dari perangkat MFA AWS mereka.

Kami menyarankan Anda mengaktifkan MFA untuk semua akun yang memiliki kata sandi konsol. MFA dirancang untuk memberikan peningkatan keamanan untuk akses konsol. Prinsipal otentikasi harus memiliki perangkat yang memancarkan kunci sensitif waktu dan harus memiliki pengetahuan tentang kredensi.

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk menambahkan MFA bagi pengguna IAM, lihat Menggunakan otentikasi multi-faktor (MFA) di Panduan Pengguna IAM. AWS

[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.5, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.6, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.6, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.14, PCI DSS v3.2. 1/8.3.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), (6), NIST.800-53.r5 IA-2 NIST.800-53.r5 IA-2 (8), PCI DSS v4.0. 1/8.4.2

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS:::Account`

AWS Configaturan: **`root-account-hardware-mfa-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda Akun AWS diaktifkan untuk menggunakan perangkat autentikasi multi-faktor perangkat keras (MFA) untuk masuk dengan kredenal pengguna root. Kontrol gagal jika

MFA perangkat keras tidak diaktifkan atau perangkat MFA virtual diizinkan untuk masuk dengan kredensi pengguna root.

MFA virtual mungkin tidak memberikan tingkat keamanan yang sama dengan perangkat MFA perangkat keras. Kami menyarankan Anda menggunakan perangkat MFA virtual hanya saat Anda menunggu persetujuan pembelian perangkat keras atau perangkat keras Anda tiba. Untuk mempelajari selengkapnya, lihat Menetapkan perangkat MFA virtual (konsol) di Panduan Pengguna IAM.

> **Note**
>
> Security Hub CSPM mengevaluasi kontrol ini berdasarkan keberadaan kredensi pengguna root (profil login) di file. Akun AWS Kontrol menghasilkan `PASSED` temuan dalam kasus-kasus berikut:
>
> - Kredensi pengguna root hadir di akun dan perangkat keras MFA diaktifkan untuk pengguna root.
> - Kredensi pengguna root tidak ada di akun.
>
> Kontrol menghasilkan `FAILED` temuan jika kredensil pengguna root ada di akun dan MFA perangkat keras tidak diaktifkan untuk pengguna root.

Remediasi

Untuk informasi tentang mengaktifkan MFA perangkat keras untuk pengguna root, Multi-factor lihat otentikasi untuk di Panduan Pengguna Pengguna root akun AWS IAM.

[IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), (15), NIST.800-53.r5 AC-3 NIST.800-53.r5 IA-5 (1), NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, 3.5.8, PCI DSS NIST.800-171.r2 v4.0. 1/8.3.6, PCI DSS v4.0. 1/8.3.7, PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.3.10.1, PCI DSS v4.0. 1/8.6.3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`RequireUppercaseCharacters`	Memerlukan setidaknya satu karakter huruf besar dalam kata sandi	Boolean	`true` atau `false`	`true`
`RequireLowercaseCharacters`	Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi	Boolean	`true` atau `false`	`true`
`RequireSymbols`	Memerlukan setidaknya satu simbol dalam kata sandi	Boolean	`true` atau `false`	`true`
`RequireNumbers`	Memerlukan setidaknya satu nomor dalam kata sandi	Boolean	`true` atau `false`	`true`
`MinimumPasswordLength`	Jumlah minimum karakter dalam kata sandi	Bilangan Bulat	8 untuk 128	8
`PasswordReusePrevention`	Jumlah rotasi kata sandi sebelum kata sandi lama dapat digunakan kembali	Bilangan Bulat	12 untuk 24	Tidak ada nilai default
`MaxPasswordAge`	Jumlah hari sebelum kedaluwarsa kata sandi	Bilangan Bulat	1 untuk 90	Tidak ada nilai default

Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM menggunakan konfigurasi yang kuat. Kontrol gagal jika kebijakan kata sandi tidak menggunakan konfigurasi yang kuat. Kecuali Anda memberikan nilai parameter kustom, Security Hub CSPM menggunakan nilai default yang disebutkan dalam tabel sebelumnya. `MaxPasswordAge`Parameter

`PasswordReusePrevention` dan tidak memiliki nilai default, jadi jika Anda mengecualikan parameter ini, Security Hub CSPM mengabaikan jumlah rotasi kata sandi dan usia kata sandi saat mengevaluasi kontrol ini.

Untuk mengaksesKonsol Manajemen AWS, pengguna IAM memerlukan kata sandi. Sebagai praktik terbaik, Security Hub CSPM sangat merekomendasikan bahwa alih-alih membuat pengguna IAM, Anda menggunakan federasi. Federasi memungkinkan pengguna untuk menggunakan kredensi perusahaan mereka yang ada untuk masuk ke. Konsol Manajemen AWS Gunakan AWS IAM Identity Center (IAM Identity Center) untuk membuat atau menyatukan pengguna, dan kemudian mengambil peran IAM ke dalam akun.

Untuk mempelajari selengkapnya tentang penyedia identitas dan federasi, lihat Penyedia identitas dan federasi di Panduan Pengguna IAM. Untuk mempelajari selengkapnya tentang Pusat Identitas IAM, lihat Panduan AWS IAM Identity Center Pengguna.

Jika Anda perlu menggunakan pengguna IAM, Security Hub CSPM merekomendasikan agar Anda menerapkan pembuatan kata sandi pengguna yang kuat. Anda dapat menetapkan kebijakan kata sandi Akun AWS untuk menentukan persyaratan kompleksitas dan periode rotasi wajib untuk kata sandi. Saat Anda membuat atau mengubah kebijakan kata sandi, sebagian besar pengaturan kebijakan kata sandi diberlakukan saat pengguna mengubah kata sandi mereka berikutnya. Beberapa pengaturan diberlakukan segera.

Remediasi

Untuk memperbarui kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM.

[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.3, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3),, NIST.800-53.r5 AC-3 (15) NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7),, NIST.800-171.r2 3.1.2 NIST.800-53.r5 AC-6, PCI DSS v3.2. 1/8.1.4, PCI DSS v4.0. 1/8.2.6

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: **`iam-user-unused-credentials-check`**

Jenis jadwal: Periodik

Parameter:

- `maxCredentialUsageAge`: `90` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kata sandi atau kunci akses aktif yang belum digunakan selama 90 hari.

Pengguna IAM dapat mengakses AWS sumber daya menggunakan berbagai jenis kredensyal, seperti kata sandi atau kunci akses.

Security Hub CSPM merekomendasikan agar Anda menghapus atau menonaktifkan semua kredensyal yang tidak digunakan selama 90 hari atau lebih. Menonaktifkan atau menghapus kredensil yang tidak perlu mengurangi jendela peluang untuk kredensil yang terkait dengan akun yang disusupi atau ditinggalkan untuk digunakan.

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Saat Anda melihat informasi pengguna di konsol IAM, ada kolom untuk usia kunci Access, Usia kata sandi, dan Aktivitas terakhir. Jika nilai di salah satu kolom ini lebih besar dari 90 hari, buat kredensyal untuk pengguna tersebut tidak aktif.

Anda juga dapat menggunakan laporan kredensi untuk memantau pengguna dan mengidentifikasi mereka yang tidak memiliki aktivitas selama 90 hari atau lebih. Anda dapat mengunduh laporan kredensi dalam `.csv` format dari konsol IAM.

Setelah Anda mengidentifikasi akun yang tidak aktif atau kredensi yang tidak digunakan, nonaktifkan akun tersebut. Untuk petunjuk, lihat Membuat, mengubah, atau menghapus kata sandi pengguna (konsol) IAM di Panduan Pengguna IAM.

[IAM.9] MFA harus diaktifkan untuk pengguna root

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.4, PCI DSS v3.2. 1/8.3.1, PCI DSS v4.0. 1/8.4.2, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.5, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.5, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.13, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`root-account-mfa-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah otentikasi multi-faktor (MFA) diaktifkan untuk pengguna root IAM untuk masuk Akun AWS ke file. Konsol Manajemen AWS Kontrol gagal jika MFA tidak diaktifkan untuk pengguna root akun.

Pengguna root IAM Akun AWS memiliki akses lengkap ke semua layanan dan sumber daya di akun. Jika MFA diaktifkan, pengguna harus memasukkan nama pengguna, kata sandi, dan kode otentikasi dari perangkat AWS MFA mereka untuk masuk ke. Konsol Manajemen AWS MFA menambahkan lapisan perlindungan ekstra di atas nama pengguna dan kata sandi.

Kontrol ini menghasilkan `PASSED` temuan dalam kasus-kasus berikut:

- Kredensi pengguna root ada di akun dan MFA diaktifkan untuk pengguna root.
- Kredensi pengguna root tidak ada di akun.

Kontrol menghasilkan `FAILED` temuan jika kredensil pengguna root ada di akun dan MFA tidak diaktifkan untuk pengguna root.

Remediasi

Untuk informasi tentang mengaktifkan MFA untuk pengguna root, Multi-factor lihat otentikasi untuk Pengguna root akun AWS di AWS Identity and Access Management Panduan Pengguna. Akun AWS

[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

Persyaratan terkait: NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, 3.5.8, PCI DSS NIST.800-171.r2 v3.2. 1/8.1.4, PCI DSS v3.2. 1/8.2.3, PCI DSS v3.2. 1/8.2.4, PCI DSS v3.2. 1/8.2.5

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM menggunakan konfigurasi DSS PCI minimum berikut.

- `RequireUppercaseCharacters`— Memerlukan setidaknya satu karakter huruf besar dalam kata sandi. (Default = `true`)
- `RequireLowercaseCharacters`— Memerlukan setidaknya satu karakter huruf kecil dalam kata sandi. (Default = `true`)
- `RequireNumbers`— Memerlukan setidaknya satu nomor dalam kata sandi. (Default = `true`)
- `MinimumPasswordLength`— Panjang minimum kata sandi. (Default = 7 atau lebih)
- `PasswordReusePrevention`— Jumlah kata sandi sebelum mengizinkan penggunaan kembali. (Default = 4)
- `MaxPasswordAge`— Jumlah hari sebelum kedaluwarsa kata sandi. (Default = 90)

> **Note**
>
> Pada 30 Mei 2025, Security Hub CSPM menghapus kontrol ini dari standar PCI DSS v4.0.1. PCI DSS v4.0.1 sekarang membutuhkan kata sandi untuk memiliki minimal 8 karakter. Kontrol ini terus berlaku untuk standar PCI DSS v3.2.1, yang memiliki persyaratan kata sandi yang berbeda.
> Untuk mengevaluasi kebijakan kata sandi akun terhadap persyaratan PCI DSS v4.0.1, Anda dapat menggunakan kontrol. IAM.7 Kontrol ini membutuhkan kata sandi untuk memiliki

minimal 8 karakter. Ini juga mendukung nilai khusus untuk panjang kata sandi dan parameter lainnya. IAM.7 Kontrol adalah bagian dari standar PCI DSS v4.0.1 di Security Hub CSPM.

Remediasi

Untuk memperbarui kebijakan kata sandi agar menggunakan konfigurasi yang disarankan, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM.

[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.5, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/8.3.6, PCI DSS v4.0. 1/8.6.3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu huruf besar. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Memerlukan setidaknya satu huruf besar dari alfabet Latin (A—Z).

[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.6, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/8.3.6, PCI DSS v4.0. 1/8.6.3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda. CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu huruf kecil. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Memerlukan setidaknya satu huruf kecil dari alfabet Latin (A—Z).

[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.7, NIST.800-171.r2 3.5.7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu simbol. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Password, pilih Memerlukan setidaknya satu karakter nonalfanumerik.

[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.8, NIST.800-171.r2 3.5.7, PCI DSS v4.0. 1/8.3.6, PCI DSS v4.0. 1/8.6.3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi menggunakan kumpulan karakter yang berbeda.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan setidaknya satu nomor. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk kekuatan Kata Sandi, pilih Memerlukan setidaknya satu nomor.

[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.7, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.8, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.8, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.9, NIST.800-171.r2 3.5.7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS:::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi, sebagian, menegakkan persyaratan kompleksitas kata sandi. Gunakan kebijakan kata sandi IAM untuk memastikan bahwa kata sandi setidaknya memiliki panjang tertentu.

CIS merekomendasikan bahwa kebijakan kata sandi memerlukan panjang kata sandi minimum 14 karakter. Menyetel kebijakan kompleksitas kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk panjang minimum Kata Sandi, masukkan **14** atau nomor yang lebih besar.

[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.8, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.9, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.9, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.10, NIST.800-171.r2 3.5.8, PCI DSS v4.0. 1/8.3.7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS:::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah jumlah kata sandi yang harus diingat diatur ke 24. Kontrol gagal jika nilainya tidak 24.

Kebijakan kata sandi IAM dapat mencegah penggunaan kembali kata sandi yang diberikan oleh pengguna yang sama.

CIS merekomendasikan agar kebijakan kata sandi mencegah penggunaan kembali kata sandi. Mencegah penggunaan kembali kata sandi meningkatkan ketahanan akun terhadap upaya login brute force.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk Mencegah penggunaan kembali kata sandi, masukkan**24**.

[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.11, PCI DSS v4.0. 1/8.3.9, PCI DSS v4.0. 1/8.3.10.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-password-policy`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kebijakan kata sandi IAM dapat mengharuskan kata sandi diputar atau kedaluwarsa setelah beberapa hari tertentu.

CIS merekomendasikan agar kebijakan kata sandi kedaluwarsa kata sandi setelah 90 hari atau kurang. Mengurangi masa pakai kata sandi meningkatkan ketahanan akun terhadap upaya login brute force. Memerlukan perubahan kata sandi reguler juga membantu dalam skenario berikut:

- Kata sandi dapat dicuri atau dikompromikan tanpa sepengetahuan Anda. Ini dapat terjadi melalui kompromi sistem, kerentanan perangkat lunak, atau ancaman internal.

- Filter web perusahaan dan pemerintah tertentu atau server proxy dapat mencegat dan merekam lalu lintas bahkan jika itu dienkripsi.
- Banyak orang menggunakan kata sandi yang sama untuk banyak sistem seperti pekerjaan, email, dan pribadi.
- Workstation pengguna akhir yang dikompromikan mungkin memiliki keystroke logger.

Remediasi

Untuk mengubah kebijakan kata sandi, lihat Menyetel kebijakan kata sandi akun untuk pengguna IAM di Panduan Pengguna IAM. Untuk Aktifkan kedaluwarsa kata sandi, masukkan **`90`** atau nomor yang lebih kecil.

[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.16, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.17, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.17, Tolok Ukur Yayasan AWS CIS v1.2. 0/1.20, NIST.800-171.r2 3.1.2, PCI DSS v4.0. 1/12.10.3

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`iam-policy-in-use`**

Jenis jadwal: Periodik

Parameter:

- `policyARN`: `arn:`*`partition`*`:iam::aws:policy/AWSSupportAccess` (tidak dapat disesuaikan)
- `policyUsageType`: `ANY` (tidak dapat disesuaikan)

AWSmenyediakan pusat dukungan yang dapat digunakan untuk pemberitahuan dan respons insiden, serta dukungan teknis dan layanan pelanggan.

Buat peran IAM untuk memungkinkan pengguna yang berwenang mengelola insiden dengan SupportAWS. Dengan menerapkan hak istimewa terkecil untuk kontrol akses, peran IAM akan

memerlukan kebijakan IAM yang sesuai untuk memungkinkan akses pusat dukungan untuk mengelola insiden dengan. Dukungan

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengatasi masalah ini, buat peran untuk memungkinkan pengguna yang berwenang mengelola Dukungan insiden.

Untuk membuat peran yang akan digunakanDukunganakses

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi IAM, pilih Peran, lalu pilih Buat peran.
3. Untuk tipe Peran, pilih Yang Lain Akun AWS.
4. Untuk ID Akun, masukkan Akun AWS ID yang Akun AWS ingin Anda berikan akses ke sumber daya Anda.

   Jika pengguna atau grup yang akan mengambil peran ini berada di akun yang sama, maka masukkan nomor akun lokal.

   > **Note**
   >
   > Administrator akun yang ditentukan dapat memberikan izin untuk mengasumsikan peran ini kepada setiap pengguna dalam akun tersebut. Untuk melakukannya, administrator melampirkan kebijakan kepada pengguna atau grup yang memberikan izin untuk tindakan `sts:AssumeRole`. Dalam kebijakan itu, sumber daya harus menjadi peran ARN.

5. Pilih Berikutnya: Izin.
6. Cari kebijakan terkelolaAWSSupportAccess.

7. Pilih kotak centang untuk kebijakan `AWSSupportAccess` terkelola.
8. Pilih Berikutnya: Tanda.
9. (Opsional) Untuk menambahkan metadata ke peran, lampirkan tag sebagai pasangan nilai kunci.

   Untuk informasi selengkapnya tentang penggunaan tag di IAM, lihat Menandai pengguna dan peran IAM di Panduan Pengguna IAM.
10. Pilih Berikutnya: Tinjauan.
11. Untuk Nama peran, masukkan nama peran Anda.

    Nama peran harus unik di dalam diri AndaAkun AWS. Mereka tidak peka huruf besar/kecil.
12. (Opsional) Untuk Deskripsi peran, masukkan deskripsi.
13. Tinjau peran, lalu pilih Buat peran.

[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8), NIST.800-53.r5 IA-2 3.3.8, NIST.800-171.r2 3.5.3, NIST.800-171.r2 NIST.800-171.r2 3.5.4, 3.7.5, PCI DSS v3.2. NIST.800-171.r2 1/8.3.1, PCI DSS v4.0. 1/8.4.2,

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: **`iam-user-mfa-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM mengaktifkan otentikasi multi-faktor (MFA).

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat

menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk menambahkan MFA bagi pengguna IAM, lihat Mengaktifkan perangkat MFA untuk pengguna di AWS Panduan Pengguna IAM.

[IAM.20] Hindari penggunaan pengguna root

Important

Security Hub CSPM menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Log perubahan untuk kontrol CSPM Security Hub.

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v1.2. 0/1.1

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: `use-of-root-account-test` (aturan CSPM Security Hub kustom)

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah a Akun AWS memiliki batasan pada penggunaan pengguna root. Kontrol mengevaluasi sumber daya berikut:

- Topik Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrailjalan setapak
- Filter metrik yang terkait dengan CloudTrail jejak
- CloudWatch Alarm Amazon berdasarkan filter

Pemeriksaan ini menghasilkan `FAILED` temuan jika satu atau beberapa pernyataan berikut benar:

- Tidak ada CloudTrail jejak di akun.
- CloudTrail Jejak diaktifkan, tetapi tidak dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis.
- CloudTrail Jejak diaktifkan, tetapi tidak terkait dengan grup CloudWatch log Log.
- Filter metrik yang tepat yang ditentukan oleh Center for Internet Security (CIS) tidak digunakan. Filter metrik yang ditentukan adalah`'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`.
- Tidak ada CloudWatch alarm berdasarkan filter metrik di akun.
- CloudWatch alarm yang dikonfigurasi untuk mengirim notifikasi ke topik SNS terkait tidak dipicu berdasarkan kondisi alarm.
- Topik SNS tidak sesuai dengan batasan untuk mengirim pesan ke topik SNS.
- Topik SNS tidak memiliki setidaknya satu pelanggan.

Pemeriksaan ini menghasilkan status kontrol `NO_DATA` jika satu atau beberapa pernyataan berikut benar:

- Jejak multi-wilayah berbasis di Wilayah yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan di Wilayah tempat jejak tersebut berada.
- Jejak multi-wilayah milik akun yang berbeda. Security Hub CSPM hanya dapat menghasilkan temuan untuk akun yang memiliki jejak.

Pemeriksaan ini menghasilkan status kontrol `WARNING` jika satu atau beberapa pernyataan berikut benar:

- Akun saat ini tidak memiliki topik SNS yang direferensikan dalam alarm. CloudWatch
- Akun saat ini tidak memiliki akses ke topik SNS saat menjalankan `ListSubscriptionsByTopic` SNS API.

> **Note**
>
> Sebaiknya gunakan jejak organisasi untuk mencatat peristiwa dari banyak akun di suatu organisasi. Jejak organisasi adalah jalur Multi-wilayah secara default dan hanya dapat dikelola oleh akun AWS Organizations manajemen atau akun administrator yang CloudTrail didelegasikan. Menggunakan jejak organisasi menghasilkan status kontrol NO_DATA untuk

kontrol yang dievaluasi di akun anggota organisasi. Di akun anggota, Security Hub CSPM hanya menghasilkan temuan untuk sumber daya milik anggota. Temuan yang berkaitan dengan jejak organisasi dihasilkan di akun pemilik sumber daya. Anda dapat melihat temuan ini di akun administrator delegasi CSPM Security Hub menggunakan agregasi lintas wilayah.

Sebagai praktik terbaik, gunakan kredensil pengguna root Anda hanya jika diperlukan untuk melakukan tugas manajemen akun dan layanan. Terapkan kebijakan IAM secara langsung ke grup dan peran tetapi tidak untuk pengguna. Untuk petunjuk cara menyiapkan administrator untuk penggunaan sehari-hari, lihat Membuat pengguna dan grup admin IAM pertama Anda di Panduan Pengguna IAM.

Remediasi

Langkah-langkah untuk mengatasi masalah ini termasuk menyiapkan topik Amazon SNS, jejak, CloudTrail filter metrik, dan alarm untuk filter metrik.

Untuk membuat topik Amazon SNS

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Buat topik Amazon SNS yang menerima semua alarm CIS.

   Buat setidaknya satu pelanggan untuk topik tersebut. Untuk informasi lebih lanjut, lihat Memulai dengan Amazon SNS di Panduan Developer Amazon Simple Notification Service.

Selanjutnya, siapkan aktif CloudTrail yang berlaku untuk semua Wilayah. Untuk melakukannya, ikuti langkah-langkah remediasi dithe section called “[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis”.

Catat nama grup CloudWatch log Log yang Anda kaitkan dengan CloudTrail jejak. Anda membuat filter metrik untuk grup log tersebut.

Terakhir, buat filter metrik dan alarm.

Untuk membuat filter metrik dan alarm

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Pada panel navigasi, pilih Grup log.

3. Pilih kotak centang untuk grup CloudWatch log Log yang terkait dengan CloudTrail jejak yang Anda buat.
4. Dari Tindakan, pilih Buat Filter Metrik.
5. Di bawah Tentukan pola, lakukan hal berikut:

    a. Salin pola berikut dan kemudian tempelkan ke bidang Filter Pattern.

    ```
    {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
     $.eventType !="AwsServiceEvent"}
    ```

    b. Pilih Berikutnya.
6. Di bawah Tetapkan Metrik, lakukan hal berikut:

    a. Di Nama filter, masukkan nama untuk filter metrik Anda.

    b. Untuk Metric Namespace, masukkan. **`LogMetrics`**

    Jika Anda menggunakan namespace yang sama untuk semua filter metrik log CIS Anda, maka semua metrik Tolok Ukur CIS dikelompokkan bersama.

    c. Untuk Nama Metrik, masukkan nama untuk metrik. Ingat nama metrik. Anda harus memilih metrik saat membuat alarm.

    d. Untuk Metric value (Nilai metrik), masukkan **1**.

    e. Pilih Berikutnya.
7. Di bawah Tinjau dan buat, verifikasi informasi yang Anda berikan untuk filter metrik baru. Kemudian, pilih Buat filter metrik.
8. Di panel navigasi, pilih Grup log, lalu pilih filter yang Anda buat di bawah Filter metrik.
9. Pilih kotak centang untuk filter. Pilih Buat alarm.
10. Di bawah Tentukan metrik dan kondisi, lakukan hal berikut:

    a. Di bawah Kondisi, untuk Ambang Batas, pilih Statis.

    b. Untuk Tentukan kondisi alarm, pilih Greater/Equal.

    c. Untuk Tentukan nilai ambang batas, masukkan**1**.

    d. Pilih Berikutnya.
11. Di bawah Konfigurasi tindakan, lakukan hal berikut:

    a. Di bawah Pemicu status alarm, pilih Dalam alarm.

    b. Di bawah Pilih topik SNS, pilih Pilih topik SNS yang sudah ada.

c. Untuk Kirim pemberitahuan ke, masukkan nama topik SNS yang Anda buat di prosedur sebelumnya.

d. Pilih Berikutnya.

12. Di bawah Tambahkan nama dan deskripsi, masukkan Nama dan Deskripsi untuk alarm, seperti**`CIS-1.1-RootAccountUsage`**. Lalu pilih Selanjutnya.
13. Di bawah Pratinjau dan buat, tinjau konfigurasi alarm. Kemudian pilih Buat alarm.

[IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), (7),,, NIST.800-53.r5 AC-3 (10) NIST.800-53.r5 AC-5 NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (2), NIST.800-53.r5 AC-6 NIST.800-53.r5 AC-6 (3), NIST.800-171.r2 3.1.1, NIST.800-171.r2 3.1.2, NIST.800-171.r2 3.1.5, NIST.800-171.r2 3.1.7, 3.3.8, 3.3.9, 3.13.3, NIST.800-171.r2 3.13.4 NIST.800-171.r2 NIST.800-171.r2 NIST.800-171.r2

Kategori: Deteksi > Manajemen akses aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::Policy`

AWS Configaturan: **`iam-policy-no-statements-with-full-access`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludePermissionBoundaryPolicy`: `True` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan berbasis identitas IAM yang Anda buat memiliki pernyataan Izinkan yang menggunakan wildcard * untuk memberikan izin untuk semua tindakan pada layanan apa pun. Kontrol gagal jika ada pernyataan kebijakan yang disertakan `"Effect": "Allow"` dengan`"Action": "Service:*"`.

Misalnya, pernyataan berikut dalam kebijakan menghasilkan temuan yang gagal.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
```

```
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

Kontrol juga gagal jika Anda menggunakannya `"Effect": "Allow""NotAction": "service:*"`. Dalam hal ini, `NotAction` elemen menyediakan akses ke semua tindakan dalamLayanan AWS, kecuali untuk tindakan yang ditentukan dalam`NotAction`.

Kontrol ini hanya berlaku untuk kebijakan IAM yang dikelola pelanggan. Ini tidak berlaku untuk kebijakan IAM yang dikelola olehAWS.

Saat Anda menetapkan izinLayanan AWS, penting untuk mencakup tindakan IAM yang diizinkan dalam kebijakan IAM Anda. Anda harus membatasi tindakan IAM hanya pada tindakan yang diperlukan. Ini membantu Anda memberikan izin hak istimewa paling sedikit. Kebijakan yang terlalu permisif dapat menyebabkan eskalasi hak istimewa jika kebijakan tersebut dilampirkan pada prinsipal IAM yang mungkin tidak memerlukan izin.

Dalam beberapa kasus, Anda mungkin ingin mengizinkan tindakan IAM yang memiliki awalan serupa, seperti `DescribeFlowLogs` dan. `DescribeAvailabilityZones` Dalam kasus resmi ini, Anda dapat menambahkan wildcard akhiran ke awalan umum. Misalnya, `ec2:Describe*`.

Kontrol ini lolos jika Anda menggunakan tindakan IAM awalan dengan wildcard berakhiran. Misalnya, pernyataan berikut dalam kebijakan menghasilkan temuan yang dilewatkan.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

Saat mengelompokkan tindakan IAM terkait dengan cara ini, Anda juga dapat menghindari melebihi batas ukuran kebijakan IAM.

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, perekaman sumber daya global dapat diaktifkan dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat

menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Untuk mengatasi masalah ini, perbarui kebijakan IAM Anda sehingga tidak mengizinkan hak administratif "*" penuh. Untuk detail tentang cara mengedit kebijakan IAM, lihat Mengedit kebijakan IAM di Panduan Pengguna IAM.

[IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.11, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.12, Tolok Ukur Yayasan AWS CIS v1.4. 0/1.12, 3.1.2 NIST.800-171.r2

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: **`iam-user-unused-credentials-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pengguna IAM Anda memiliki kata sandi atau kunci akses aktif yang belum digunakan selama 45 hari atau lebih. Untuk melakukannya, ia memeriksa apakah `maxCredentialUsageAge` parameter AWS Config aturan sama dengan 45 atau lebih.

Pengguna dapat mengakses AWS sumber daya menggunakan berbagai jenis kredensyal, seperti kata sandi atau kunci akses.

CIS merekomendasikan agar Anda menghapus atau menonaktifkan semua kredensyal yang telah tidak digunakan selama 45 hari atau lebih. Menonaktifkan atau menghapus kredensil yang tidak perlu mengurangi jendela peluang untuk kredensil yang terkait dengan akun yang disusupi atau ditinggalkan untuk digunakan.

AWS ConfigAturan untuk kontrol ini menggunakan operasi `GenerateCredentialReport`API `GetCredentialReport`dan, yang hanya diperbarui setiap empat jam. Perubahan pada pengguna IAM dapat memakan waktu hingga empat jam untuk dapat dilihat oleh kontrol ini.

> **Note**
>
> AWS Configharus diaktifkan di semua Wilayah di mana Anda menggunakan Security Hub CSPM. Namun, Anda dapat mengaktifkan perekaman sumber daya global dalam satu Wilayah. Jika Anda hanya merekam sumber daya global dalam satu Wilayah, maka Anda dapat menonaktifkan kontrol ini di semua Wilayah kecuali Wilayah tempat Anda merekam sumber daya global.

Remediasi

Saat Anda melihat informasi pengguna di konsol IAM, ada kolom untuk usia kunci Access, Usia kata sandi, dan Aktivitas terakhir. Jika nilai di salah satu kolom ini lebih besar dari 45 hari, buat kredensyal untuk pengguna tersebut tidak aktif.

Anda juga dapat menggunakan laporan kredensi untuk memantau pengguna dan mengidentifikasi mereka yang tidak memiliki aktivitas selama 45 hari atau lebih. Anda dapat mengunduh laporan kredensi dalam `.csv` format dari konsol IAM.

Setelah Anda mengidentifikasi akun yang tidak aktif atau kredensi yang tidak digunakan, nonaktifkan akun tersebut. Untuk petunjuk, lihat Membuat, mengubah, atau menghapus kata sandi pengguna (konsol) IAM di Panduan Pengguna IAM.

[IAM.23] Penganalisis Akses IAM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AccessAnalyzer::Analyzer`

AWS Configaturan: `tagged-accessanalyzer-analyzer` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah penganalisis yang dikelola oleh AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika penganalisis tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika penganalisis tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke analyzer, lihat TagResourcedi Referensi API AWSIAM Access Analyzer.

[IAM.24] Peran IAM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::Role`

AWS Configaturan: `tagged-iam-role` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah peran AWS Identity and Access Management (IAM) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika peran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika peran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan,

Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke peran IAM, lihat Menandai sumber daya IAM di Panduan Pengguna IAM.

[IAM.25] Pengguna IAM harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IAM::User`

AWS Configaturan: `tagged-iam-user` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratanAWS.	

Kontrol ini memeriksa apakah pengguna AWS Identity and Access Management (IAM) memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika pengguna tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pengguna tidak diberi tag dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke pengguna IAM, lihat Menandai sumber daya IAM di Panduan Pengguna IAM.

[IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.18, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.19

Kategori: Identifikasi > Kepatuhan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::ServerCertificate`

AWS Configaturan: **`iam-server-certificate-expiration-check`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah sertifikat SSL/TLS server aktif yang dikelola di IAM telah kedaluwarsa. Kontrol gagal jika sertifikat SSL/TLS server yang kedaluwarsa tidak dihapus.

Untuk mengaktifkan koneksi HTTPS ke situs web atau aplikasi AndaAWS, Anda memerlukan sertifikat SSL/TLS server. Anda dapat menggunakan IAM atau AWS Certificate Manager (ACM) untuk menyimpan dan menyebarkan sertifikat server. Gunakan IAM sebagai manajer sertifikat hanya jika Anda harus mendukung koneksi HTTPS di Wilayah AWS yang tidak didukung oleh ACM. IAM mengenkripsi kunci pribadi Anda dengan aman dan menyimpan versi terenkripsinya dalam penyimpanan sertifikat IAM SSL. IAM mendukung penerapan sertifikat server di semua Wilayah, tetapi Anda harus mendapatkan sertifikat Anda dari penyedia eksternal untuk digunakan. AWS Anda tidak dapat mengunggah sertifikat ACM ke IAM. Selain itu, Anda tidak dapat mengelola sertifikat dari konsol IAM. Menghapus SSL/TLS sertifikat kedaluwarsa menghilangkan risiko bahwa sertifikat yang tidak valid disebarkan secara tidak sengaja ke sumber daya, yang dapat merusak kredibilitas aplikasi atau situs web yang mendasarinya.

Remediasi

Untuk menghapus sertifikat server dari IAM, lihat Mengelola sertifikat server di IAM di Panduan Pengguna IAM.

[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.21, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.22

Kategori: Lindungi > Manajemen akses aman > Kebijakan IAM yang aman

Tingkat keparahan: Sedang

Jenis sumber daya:`AWS::IAM::Role`,`AWS::IAM::User`, `AWS::IAM::Group`

AWS Configaturan: **`iam-policy-blacklisted-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

- “PolicyArns”: “arn:aws:iam: :aws:, arn:aws-cn:iam: :aws:, arn:aws-us-gov:iam: :awspolicy/AWSCloudShellFullAccess:” policy/AWSCloudShellFullAccess policy/AWSCloudShellFullAccess

Kontrol ini memeriksa apakah identitas IAM (pengguna, peran, atau grup) memiliki kebijakan AWS terkelola yang `AWSCloudShellFullAccess` dilampirkan. Kontrol gagal jika identitas IAM memiliki `AWSCloudShellFullAccess` kebijakan yang dilampirkan.

AWS CloudShellmenyediakan cara mudah untuk menjalankan perintah CLI terhadap. Layanan AWS Kebijakan AWS terkelola `AWSCloudShellFullAccess` menyediakan akses penuh CloudShell, yang memungkinkan kemampuan mengunggah dan mengunduh file antara sistem lokal pengguna dan CloudShell lingkungan. Dalam CloudShell lingkungan, pengguna memiliki izin sudo, dan dapat mengakses internet. Akibatnya, melampirkan kebijakan terkelola ini ke identitas IAM memberi mereka kemampuan untuk menginstal perangkat lunak transfer file dan memindahkan data dari CloudShell ke server internet eksternal. Sebaiknya ikuti prinsip hak istimewa paling sedikit dan melampirkan izin yang lebih sempit ke identitas IAM Anda.

Remediasi

Untuk melepaskan *`AWSCloudShellFullAccess`* kebijakan dari identitas IAM, lihat Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna IAM.

[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/1.19, Tolok Ukur Yayasan AWS CIS v3.0. 0/1.20

Kategori: Deteksi > Layanan deteksi > Pemantauan penggunaan istimewa

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::AccessAnalyzer::Analyzer`

AWS Configaturan: **`iam-external-access-analyzer-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah Akun AWS penganalisis akses eksternal IAM Access Analyzer diaktifkan. Kontrol gagal jika akun tidak mengaktifkan penganalisis akses eksternal di pilihan Wilayah AWS Anda saat ini.

Alat analisis akses eksternal IAM Access Analyzer membantu mengidentifikasi sumber daya, seperti bucket Amazon Simple Storage Service (Amazon S3) atau peran IAM, yang dibagikan dengan entitas eksternal. Ini membantu Anda menghindari akses yang tidak diinginkan ke sumber daya dan data Anda. IAM Access Analyzer bersifat Regional dan harus diaktifkan di setiap Wilayah. Untuk mengidentifikasi sumber daya yang dibagikan dengan prinsipal eksternal, penganalisis akses menggunakan penalaran berbasis logika untuk menganalisis kebijakan berbasis sumber daya di lingkungan Anda. AWS Saat Anda membuat penganalisis akses eksternal, Anda dapat membuat dan mengaktifkannya untuk seluruh organisasi atau akun individual Anda.

> **Note**
>
> Jika akun merupakan bagian dari organisasiAWS Organizations, kontrol ini tidak memfaktorkan penganalisis akses eksternal yang menentukan organisasi sebagai zona kepercayaan dan diaktifkan untuk organisasi di Wilayah saat ini. Jika organisasi Anda menggunakan jenis konfigurasi ini, pertimbangkan untuk menonaktifkan kontrol ini untuk akun anggota individual di organisasi Anda di Wilayah.

Remediasi

Untuk informasi tentang mengaktifkan penganalisis akses eksternal di Wilayah tertentu, lihat Memulai IAM Access Analyzer di Panduan Pengguna IAM. Anda harus mengaktifkan penganalisis di setiap Wilayah tempat Anda ingin memantau akses ke sumber daya Anda.

Kontrol CSPM Security Hub untuk Amazon Inspector

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Inspector.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/11.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`inspector-ec2-scan-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemindaian Amazon Inspector EC2 diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian Amazon Inspector EC2 dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak mengaktifkan pemindaian EC2.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur pemindaian EC2 untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian Amazon Inspector EC2. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

Pemindaian Amazon Inspector EC2 mengekstrak metadata dari instans Amazon Elastic Compute Cloud (Amazon EC2), lalu membandingkan metadata ini dengan aturan yang dikumpulkan dari penasihat keamanan untuk menghasilkan temuan. Amazon Inspector memindai instans untuk kerentanan paket dan masalah jangkauan jaringan. Untuk informasi tentang sistem operasi yang didukung, termasuk sistem operasi mana yang dapat dipindai tanpa agen SSM, lihat Sistem operasi yang didukung: Pemindaian Amazon EC2.

Remediasi

Untuk mengaktifkan pemindaian Amazon Inspector EC2, lihat Mengaktifkan pemindaian di Panduan Pengguna Amazon Inspector.

[Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/11.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`inspector-ecr-scan-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemindaian Amazon Inspector ECR diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian Amazon Inspector ECR dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak mengaktifkan pemindaian ECR.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur pemindaian ECR untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian Amazon Inspector ECR. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

Amazon Inspector memindai gambar kontainer yang disimpan di Amazon Elastic Container Registry (Amazon ECR) untuk mencari kerentanan perangkat lunak untuk menghasilkan temuan kerentanan paket. Saat mengaktifkan pemindaian Amazon Inspector untuk Amazon ECR, Anda menetapkan Amazon Inspector sebagai layanan pemindaian pilihan untuk registri pribadi Anda. Ini menggantikan pemindaian dasar, yang disediakan tanpa biaya oleh Amazon ECR, dengan pemindaian yang disempurnakan, yang disediakan dan ditagih melalui Amazon Inspector. Pemindaian yang disempurnakan memberi Anda manfaat pemindaian kerentanan untuk sistem operasi dan paket bahasa pemrograman di tingkat registri. Anda dapat meninjau temuan yang ditemukan menggunakan pemindaian yang disempurnakan pada tingkat gambar, untuk setiap lapisan gambar, di konsol Amazon ECR. Selain itu, Anda dapat meninjau dan bekerja dengan temuan ini di layanan lain yang

tidak tersedia untuk temuan pemindaian dasar, termasuk AWS Security Hub CSPM dan Amazon EventBridge.

Remediasi

Untuk mengaktifkan pemindaian Amazon Inspector ECR, lihat Mengaktifkan pemindaian di Panduan Pengguna Amazon Inspector.

[Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/6.2.4, PCI DSS v4.0. 1/6.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`inspector-lambda-code-scan-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemindaian kode Amazon Inspector Lambda diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian kode Amazon Inspector Lambda dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak mengaktifkan pemindaian kode Lambda.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur pemindaian kode Lambda untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian kode Amazon Inspector Lambda. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

Pemindaian kode Amazon Inspector Lambda memindai kode aplikasi khusus dalam AWS Lambda fungsi untuk kerentanan kode berdasarkan praktik terbaik keamanan. AWS Pemindaian kode Lambda dapat mendeteksi kekurangan injeksi, kebocoran data, kriptografi lemah, atau enkripsi

yang hilang dalam kode Anda. Fitur ini Wilayah AWShanya tersedia secara spesifik. Anda dapat mengaktifkan pemindaian kode Lambda bersama dengan pemindaian standar Lambda (lihat). [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan

Remediasi

Untuk mengaktifkan pemindaian kode Amazon Inspector Lambda, lihat Mengaktifkan pemindaian di Panduan Pengguna Amazon Inspector.

[Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan

Persyaratan terkait: PCI DSS v4.0. 1/6.2.4, PCI DSS v4.0. 1/6.3.1

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS:::Account`

AWS Configaturan: **`inspector-lambda-standard-scan-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah pemindaian standar Amazon Inspector Lambda diaktifkan. Untuk akun mandiri, kontrol gagal jika pemindaian standar Amazon Inspector Lambda dinonaktifkan di akun. Di lingkungan multi-akun, kontrol gagal jika akun administrator Amazon Inspector yang didelegasikan dan semua akun anggota tidak mengaktifkan pemindaian standar Lambda.

Dalam lingkungan multi-akun, kontrol menghasilkan temuan hanya di akun administrator Amazon Inspector yang didelegasikan. Hanya administrator yang didelegasikan yang dapat mengaktifkan atau menonaktifkan fitur pemindaian standar Lambda untuk akun anggota di organisasi. Akun anggota Amazon Inspector tidak dapat mengubah konfigurasi ini dari akun mereka. Kontrol ini menghasilkan `FAILED` temuan jika administrator yang didelegasikan memiliki akun anggota yang ditangguhkan yang tidak mengaktifkan pemindaian standar Amazon Inspector Lambda. Untuk menerima `PASSED` temuan, administrator yang didelegasikan harus memisahkan akun yang ditangguhkan ini di Amazon Inspector.

Pemindaian standar Amazon Inspector Lambda mengidentifikasi kerentanan perangkat lunak dalam dependensi paket aplikasi yang Anda tambahkan ke kode fungsi dan lapisan Anda. AWS Lambda

Jika Amazon Inspector mendeteksi kerentanan dalam dependensi paket aplikasi fungsi Lambda Anda, Amazon Inspector menghasilkan temuan tipe terperinci. `Package Vulnerability` Anda dapat mengaktifkan pemindaian kode Lambda bersama dengan pemindaian standar Lambda (lihat). [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan

Remediasi

Untuk mengaktifkan pemindaian standar Amazon Inspector Lambda, lihat Mengaktifkan pemindaian di Panduan Pengguna Amazon Inspector.

Kontrol CSPM Security Hub untukAWS IoT

AWS Security Hub CSPMKontrol ini mengevaluasi AWS IoT layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::SecurityProfile`

AWS Configaturan: `tagged-iot-securityprofile` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratanAWS.	

Kontrol ini memeriksa apakah profil AWS IoT Device Defender keamanan memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika profil keamanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil keamanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke profil AWS IoT Device Defender keamanan, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

[IoT.2]AWS IoT Coretindakan mitigasi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::MitigationAction`

AWS Configaturan: `tagged-iot-mitigationaction` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah tindakan AWS IoT Core mitigasi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika tindakan mitigasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredTagKeys` Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tindakan mitigasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke tindakan AWS IoT Core mitigasi, lihat Menandai AWS IoT sumber daya Anda di Panduan Pengembang. AWS IoT

[IoT.3]AWS IoT Coredimensi harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Dimension`

AWS Configaturan: `tagged-iot-dimension` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratanAWS.	

Kontrol ini memeriksa apakah AWS IoT Core dimensi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika dimensi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika dimensi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core dimensi, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

[IoT.4]AWS IoT Coreotorisasi harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Authorizer`

AWS Configaturan: `tagged-iot-authorizer` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah AWS IoT Core otorisasi memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika otorisasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika otorisasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core otorisasi, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

[IoT.5]AWS IoT Corealias peran harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::RoleAlias`

AWS Configaturan: `tagged-iot-rolealias` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
			persyaratanAWS.	

Kontrol ini memeriksa apakah alias AWS IoT Core peran memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika alias peran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alias peran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alias AWS IoT Core peran, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

[IoT.6]AWS IoT Corekebijakan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoT::Policy`

AWS Configaturan: `tagged-iot-policy` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah AWS IoT Core kebijakan memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika kebijakan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke AWS IoT Core kebijakan, lihat Menandai AWS IoT sumber daya Anda di Panduan AWS IoT Pengembang.

Kontrol CSPM Security Hub untukAWSIoT SiteWise

AWS Security Hub CSPMKontrol ini mengevaluasi SiteWise layanan dan AWS sumber daya IoT.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::AssetModel`

AWS Configaturan: `iotsitewise-asset-model-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah model SiteWise aset AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika model aset tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika model aset tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke model SiteWise aset AWS IoT, lihat Menandai AWS IoT SiteWise sumber daya Anda di AWS IoT SiteWisePanduan Pengguna.

[IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::Dashboard`

AWS Configaturan: `iotsitewise-dashboard-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise dasbor AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika dasbor tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika dasbor tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan

tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke SiteWise dasbor AWS IoT, lihat Menandai AWS IoT SiteWise sumber daya Anda di AWS IoT SiteWisePanduan Pengguna.

[IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::Gateway`

AWS Configaturan: `iotsitewise-gateway-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise gateway AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika gateway tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gateway tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke SiteWise gateway AWS IoT, lihat Menandai AWS IoT SiteWise sumber daya Anda di AWS IoT SiteWisePanduan Pengguna.

[IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::Portal`

AWS Configaturan: `iotsitewise-portal-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise portal AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika portal tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika portal tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan

tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke SiteWise portal AWS IoT, lihat Menandai AWS IoT SiteWise sumber daya Anda di AWS IoT SiteWisePanduan Pengguna.

[IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTSiteWise::Project`

AWS Configaturan: `iotsitewise-project-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah SiteWise proyek AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika proyek tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika proyek tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke SiteWise proyek AWS IoT, lihat Menandai AWS IoT SiteWise sumber daya Anda di AWS IoT SiteWisePanduan Pengguna.

Kontrol CSPM Security Hub untukAWSIoT TwinMaker

AWS Security Hub CSPMKontrol ini mengevaluasi TwinMaker layanan dan AWS sumber daya IoT.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTTwinMaker::SyncJob`

AWS Configaturan: `iottwinmaker-sync-job-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah pekerjaan TwinMaker sinkronisasi AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika pekerjaan sinkronisasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya

memeriksa keberadaan kunci tag dan gagal jika pekerjaan sinkronisasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke pekerjaan TwinMaker sinkronisasi AWS IoT, lihat TagResourcedi AWS IoT TwinMakerPanduan Pengguna.

[IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTTwinMaker::Workspace`

AWS Configaturan: `iottwinmaker-workspace-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah TwinMaker ruang kerja AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika ruang kerja tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika ruang kerja tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke TwinMaker ruang kerja AWS IoT, lihat TagResourcedi Panduan Pengguna. AWS IoT TwinMaker

[IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTTwinMaker::Scene`

AWS Configaturan: `iottwinmaker-scene-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah TwinMaker adegan AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika adegan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika adegan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke TwinMaker adegan AWS IoT, lihat TagResourcedi AWS IoT TwinMakerPanduan Pengguna.

[IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTTwinMaker::Entity`

AWS Configaturan: `iottwinmaker-entity-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah TwinMaker entitas AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika entitas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika entitas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke TwinMaker entitas AWS IoT, lihat TagResourcedi AWS IoT TwinMakerPanduan Pengguna.

Kontrol CSPM Security Hub untukAWSIoT Wireless

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan AWS sumber daya IoT Wireless.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTWireless::MulticastGroup`

AWS Configaturan: `iotwireless-multicast-group-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah grup multicast Nirkabel AWS IoT memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika grup multicast tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter. `requiredKeyTags` Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa

keberadaan kunci tag dan gagal jika grup multicast tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke grup multicast Nirkabel AWS IoT, lihat Menandai sumber daya AWS IoT Wireless Anda di Panduan Pengembang. AWS IoT Wireless

[IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTWireless::ServiceProfile`

AWS Configaturan: `iotwireless-service-profile-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah profil layanan AWS IoT Wireless memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika profil layanan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil layanan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke profil layanan Nirkabel AWS IoT, lihat Menandai sumber daya AWS IoT Wireless Anda di Panduan AWS IoT WirelessPengembang.

[IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IoTWireless::FuotaTask`

AWS Configaturan: `iotwireless-fuota-task-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah tugas pembaruan firmware AWS IoT Wireless over-the-air (FUOTA) memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika tugas FUOTA tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika tugas FUOTA tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke tugas FUOTA Nirkabel AWS IoT, lihat Menandai sumber daya AWS IoT Wireless Anda di AWS IoT Wireless Panduan Pengembang.

Kontrol CSPM Security Hub untuk Amazon IVS

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Interactive Video Service (IVS).

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[IVS.1] Pasangan kunci pemutaran IVS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IVS::PlaybackKeyPair`

AWS Configaturan: `ivs-playback-key-pair-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah key pair Amazon IVS playback memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika playback key pair tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika key pair playback tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke key pair pemutaran IVS, lihat TagResourcedi Referensi API Real-Time Streaming Amazon IVS.

[IVS.2] Konfigurasi perekaman IVS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IVS::RecordingConfiguration`

AWS Configaturan: `ivs-recording configuration-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah konfigurasi perekaman Amazon IVS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika konfigurasi perekaman tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam

parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konfigurasi perekaman tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke konfigurasi perekaman IVS, lihat TagResourcedi Referensi API Real-Time Streaming Amazon IVS.

[IVS.3] Saluran IVS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::IVS::Channel`

AWS Configaturan: `ivs-channel-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah saluran Amazon IVS memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika saluran tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika saluran tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke saluran IVS, lihat TagResourcedi Referensi API Real-Time Streaming Amazon IVS.

Kontrol CSPM Security Hub untuk Amazon Keyspaces

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Keyspaces.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Cassandra::Keyspace`

AWS Configaturan: `cassandra-keyspace-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah ruang kunci Amazon Keyspaces memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredKeyTags` Kontrol gagal jika ruang kunci tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika ruang kunci tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke ruang kunci Amazon Keyspaces, lihat Menambahkan tag ke ruang kunci di Panduan Pengembang Amazon Keyspaces.

Kontrol CSPM Security Hub untuk Kinesis

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Kinesis.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Kinesis::Stream`

AWS Configaturan: kinesis-stream-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Kinesis Data Streams dienkripsi saat istirahat dengan enkripsi sisi server. Kontrol ini gagal jika aliran Kinesis tidak dienkripsi saat istirahat dengan enkripsi sisi server.

Server-side enkripsi adalah fitur di Amazon Kinesis Data Streams yang secara otomatis mengenkripsi data sebelum diam dengan menggunakan file. AWS KMS key Data dienkripsi sebelum ditulis ke lapisan penyimpanan aliran Kinesis, dan didekripsi setelah diambil dari penyimpanan. Akibatnya, data Anda dienkripsi saat istirahat dalam layanan Amazon Kinesis Data Streams.

Remediasi

Untuk informasi tentang mengaktifkan enkripsi sisi server untuk aliran Kinesis, lihat Bagaimana cara memulai enkripsi sisi server? di Panduan Pengembang Amazon Kinesis.

[Kinesis.2] Aliran Kinesis harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Kinesis::Stream`

AWS Configaturan: `tagged-kinesis-stream` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah aliran data Amazon Kinesis memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika aliran data tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aliran data tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke aliran data Kinesis, lihat Menandai aliran Anda di Amazon Kinesis Data Streams di Panduan Pengembang Amazon Kinesis.

[Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Kinesis::Stream`

AWS Configaturan: kinesis-stream-backup-retention-check

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`minimumBackupRetentionPeriod`	Jumlah jam minimum data harus disimpan.	String	24 hingga 8760	168

Kontrol ini memeriksa apakah aliran data Amazon Kinesis memiliki periode retensi data yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika periode retensi data kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode penyimpanan data, Security Hub CSPM menggunakan nilai default 168 jam.

Dalam Kinesis Data Streams, aliran data adalah urutan urutan catatan data yang dimaksudkan untuk ditulis dan dibaca secara real time. Catatan data disimpan dalam pecahan di aliran Anda untuk sementara. Periode waktu dari saat catatan ditambahkan ke saat tidak lagi dapat diakses disebut periode retensi. Kinesis Data Streams segera membuat catatan yang lebih tua dari periode retensi baru tidak dapat diakses setelah mengurangi periode retensi. Misalnya, mengubah periode retensi dari 24 jam menjadi 48 jam berarti rekaman yang ditambahkan ke aliran 23 jam 55 menit sebelumnya masih tersedia setelah 24 jam.

Remediasi

Untuk mengubah periode retensi cadangan untuk Kinesis Data Streams, lihat Mengubah periode retensi data di Panduan Pengembang Amazon Kinesis Data Streams.

Kontrol CSPM Security Hub untukAWS KMS

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Key Management Service (AWS KMS) layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::IAM::Policy`

AWS Configaturan: iam-customer-policy-blocked-kms-actions

Jenis jadwal: Perubahan dipicu

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(tidak dapat disesuaikan)
- `excludePermissionBoundaryPolicy`: `True` (tidak dapat disesuaikan)

Memeriksa apakah versi default dari kebijakan terkelola pelanggan IAM mengizinkan prinsipal untuk menggunakan tindakan AWS KMS dekripsi pada semua sumber daya. Kontrol gagal jika kebijakan cukup terbuka untuk mengizinkan `kms:Decrypt` atau `kms:ReEncryptFrom` tindakan pada semua kunci KMS.

Kontrol hanya memeriksa kunci KMS dalam elemen Resource dan tidak memperhitungkan persyaratan apa pun dalam elemen Kondisi kebijakan. Selain itu, kontrol mengevaluasi kebijakan terkelola pelanggan yang terlampir dan tidak terikat. Itu tidak memeriksa kebijakan sebaris atau kebijakan AWS terkelola.

DenganAWS KMS, Anda mengontrol siapa yang dapat menggunakan kunci KMS Anda dan mendapatkan akses ke data terenkripsi Anda. Kebijakan IAM menentukan tindakan identitas (pengguna, grup, atau peran) yang dapat dilakukan pada sumber daya mana. Mengikuti praktik terbaik keamanan, AWS merekomendasikan agar Anda mengizinkan hak istimewa paling sedikit. Dengan kata lain, Anda harus memberikan identitas hanya `kms:ReEncryptFrom` izin `kms:Decrypt` atau dan hanya untuk kunci yang diperlukan untuk melakukan tugas. Jika tidak, pengguna mungkin menggunakan kunci yang tidak sesuai untuk data Anda.

Alih-alih memberikan izin untuk semua kunci, tentukan kumpulan kunci minimum yang dibutuhkan pengguna untuk mengakses data terenkripsi. Kemudian desain kebijakan yang memungkinkan pengguna untuk hanya menggunakan kunci tersebut. Misalnya, jangan izinkan `kms:Decrypt` izin pada semua kunci KMS. Sebagai gantinya, izinkan `kms:Decrypt` hanya pada kunci di Wilayah tertentu untuk akun Anda. Dengan mengadopsi prinsip hak istimewa terkecil, Anda dapat mengurangi risiko pengungkapan data Anda yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan terkelola pelanggan IAM, lihat Mengedit kebijakan yang dikelola pelanggan di Panduan Pengguna IAM. Saat mengedit kebijakan Anda, untuk `Resource` bidang tersebut, berikan Nama Sumber Daya Amazon (ARN) kunci atau kunci tertentu yang ingin Anda izinkan untuk mengaktifkan tindakan dekripsi.

[KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS

Persyaratan terkait: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (3)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Configaturan: iam-inline-policy-blocked-kms-actions

Jenis jadwal: Perubahan dipicu

Parameter:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan inline yang disematkan dalam identitas IAM Anda (peran, pengguna, atau grup) memungkinkan tindakan AWS KMS dekripsi dan enkripsi ulang pada semua kunci KMS. Kontrol gagal jika kebijakan cukup terbuka untuk mengizinkan `kms:Decrypt` atau `kms:ReEncryptFrom` tindakan pada semua kunci KMS.

Kontrol hanya memeriksa kunci KMS dalam elemen Resource dan tidak memperhitungkan persyaratan apa pun dalam elemen Kondisi kebijakan.

DenganAWS KMS, Anda mengontrol siapa yang dapat menggunakan kunci KMS Anda dan mendapatkan akses ke data terenkripsi Anda. Kebijakan IAM menentukan tindakan identitas (pengguna, grup, atau peran) yang dapat dilakukan pada sumber daya mana. Mengikuti praktik terbaik keamanan, AWS merekomendasikan agar Anda mengizinkan hak istimewa paling sedikit. Dengan kata lain, Anda harus memberikan identitas hanya izin yang mereka butuhkan dan hanya untuk kunci yang diperlukan untuk melakukan tugas. Jika tidak, pengguna mungkin menggunakan kunci yang tidak sesuai untuk data Anda.

Alih-alih memberikan izin untuk semua kunci, tentukan kumpulan kunci minimum yang dibutuhkan pengguna untuk mengakses data terenkripsi. Kemudian desain kebijakan yang memungkinkan pengguna untuk hanya menggunakan kunci tersebut. Misalnya, jangan izinkan `kms:Decrypt` izin pada semua kunci KMS. Sebagai gantinya, izinkan izin hanya pada kunci tertentu di Wilayah tertentu untuk akun Anda. Dengan mengadopsi prinsip hak istimewa terkecil, Anda dapat mengurangi risiko pengungkapan data Anda yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan sebaris IAM, lihat Mengedit kebijakan sebaris di Panduan Pengguna IAM. Saat mengedit kebijakan Anda, untuk `Resource` bidang tersebut, berikan Nama Sumber Daya Amazon (ARN) kunci atau kunci tertentu yang ingin Anda izinkan untuk mengaktifkan tindakan dekripsi.

[KMS.3]AWS KMS keystidak boleh dihapus secara tidak sengaja

Persyaratan terkait: NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::KMS::Key`

AWS Configaturan: `kms-cmk-not-scheduled-for-deletion-2` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kunci KMS dijadwalkan untuk dihapus. Kontrol gagal jika kunci KMS dijadwalkan untuk dihapus.

Kunci KMS tidak dapat dipulihkan setelah dihapus. Data yang dienkripsi di bawah kunci KMS juga tidak dapat dipulihkan secara permanen jika kunci KMS dihapus. Jika data bermakna telah dienkripsi di bawah kunci KMS yang dijadwalkan untuk dihapus, pertimbangkan untuk mendekripsi data atau mengenkripsi ulang data di bawah kunci KMS baru kecuali Anda sengaja melakukan penghapusan kriptografi.

Ketika kunci KMS dijadwalkan untuk dihapus, periode tunggu wajib diberlakukan untuk memberikan waktu untuk membalikkan penghapusan, jika dijadwalkan dalam kesalahan. Masa tunggu default adalah 30 hari, tetapi dapat dikurangi menjadi sesingkat 7 hari ketika kunci KMS dijadwalkan untuk dihapus. Selama masa tunggu, penghapusan yang dijadwalkan dapat dibatalkan dan kunci KMS tidak akan dihapus.

Untuk informasi tambahan mengenai menghapus kunci KMS, lihat Menghapus kunci KMS di Panduan Pengembang. AWS Key Management Service

Remediasi

Untuk membatalkan penghapusan kunci KMS terjadwal, lihat Untuk membatalkan penghapusan kunci di bawah Penjadwalan dan pembatalan penghapusan kunci (konsol) di Panduan Pengembang. AWS Key Management Service

[KMS.4]AWS KMSrotasi kunci harus diaktifkan

Persyaratan terkait: Tolok Ukur AWS Yayasan CIS v5.0. 0/3.6, Tolok Ukur Yayasan AWS CIS v3.0. 0/3.6, Tolok Ukur Yayasan AWS CIS v1.4. 0/3.8, Tolok Ukur Yayasan AWS CIS v1.2. 0/2.8,

NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-28 (3), PCI DSS v3.2. 1/3.6.4, PCI DSS v4.0. 1/3.7.4

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::KMS::Key`

AWS Configaturan: cmk-backing-key-rotation-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

AWS KMSmemungkinkan pelanggan untuk memutar kunci dukungan, yang merupakan bahan kunci yang disimpan AWS KMS dan diikat ke ID kunci kunci KMS. Ini adalah kunci pendukung yang digunakan untuk melakukan operasi kriptografi seperti enkripsi dan dekripsi. Rotasi kunci otomatis saat ini mempertahankan semua kunci pendukung sebelumnya sehingga dekripsi data terenkripsi dapat berlangsung secara transparan.

CIS merekomendasikan agar Anda mengaktifkan rotasi tombol KMS. Memutar kunci enkripsi membantu mengurangi dampak potensial dari kunci yang dikompromikan karena data yang dienkripsi dengan kunci baru tidak dapat diakses dengan kunci sebelumnya yang mungkin telah diekspos.

Remediasi

Untuk mengaktifkan rotasi tombol KMS, lihat Cara mengaktifkan dan menonaktifkan rotasi tombol otomatis di Panduan AWS Key Management Service Pengembang.

[KMS.5] Kunci KMS tidak boleh diakses publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::KMS::Key`

AWS Configaturan: kms-key-policy-no-public-access

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa AWS KMS key apakah an dapat diakses publik. Kontrol gagal jika kunci KMS dapat diakses publik.

Menerapkan akses hak istimewa paling sedikit sangat penting untuk mengurangi risiko keamanan dan dampak kesalahan atau niat jahat. Jika kebijakan kunci untuk AWS KMS key mengizinkan akses dari akun eksternal, pihak ketiga mungkin dapat mengenkripsi dan mendekripsi data dengan menggunakan kunci. Hal ini dapat mengakibatkan ancaman internal atau eksternal yang mengeksfiltrasi data dari Layanan AWS yang menggunakan kunci.

> **Note**
>
> Kontrol ini juga mengembalikan `FAILED` temuan AWS KMS key jika konfigurasi Anda AWS Config mencegah merekam kebijakan kunci di Item Konfigurasi (CI) untuk kunci KMS. AWS ConfigUntuk mengisi kebijakan kunci di CI untuk kunci KMS, AWS Configperan harus memiliki akses untuk membaca kebijakan kunci menggunakan panggilan GetKeyPolicyAPI. Untuk mengatasi jenis `FAILED` temuan ini, periksa kebijakan yang dapat mencegah AWS Config peran memiliki akses baca ke kebijakan kunci untuk kunci KMS. Misalnya, periksa yang berikut ini:
>
> - Kebijakan kunci untuk kunci KMS.
> - Kebijakan kontrol layanan (SCP) dan kebijakan kontrol sumber daya (RCP) AWS Organizations yang berlaku untuk akun Anda.
> - Izin untuk AWS Config peran tersebut, jika Anda tidak menggunakan peran AWS Configterkait layanan.
>
> Selain itu, kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan `PASSED` temuan, kondisi dalam kebijakan kunci hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat Variabel dan tag di Panduan AWS Identity and Access Management Pengguna.

Remediasi

Untuk informasi tentang memperbarui kebijakan kunciAWS KMS key, lihat Kebijakan kunci AWS KMS di Panduan AWS Key Management Service Pengembang.

Kontrol CSPM Hub Keamanan untuk AWS Lambda

AWS Security Hub CSPM Kontrol ini mengevaluasi AWS Lambda layanan dan sumber daya. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, PCI DSS v4.0. 1/7.2.1

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: lambda-function-public-access-prohibited

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan berbasis sumber daya fungsi Lambda melarang akses publik di luar akun Anda. Kontrol gagal jika akses publik diizinkan. Kontrol juga gagal jika fungsi Lambda dipanggil dari Amazon S3, dan kebijakan tidak menyertakan kondisi untuk membatasi akses publik, seperti. `AWS:SourceAccount` Sebaiknya gunakan kondisi S3 lainnya bersama dengan `AWS:SourceAccount` kebijakan bucket Anda untuk akses yang lebih halus.

> **Note**
>
> Kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan tem `PASSED` uan, kondisi dalam kebijakan untuk fungsi Lambda hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat Variabel dan tag di Panduan AWS Identity and Access Management Pengguna.

Fungsi Lambda seharusnya tidak dapat diakses publik, karena ini dapat memungkinkan akses yang tidak diinginkan ke kode fungsi Anda.

Remediasi

Untuk mengatasi masalah ini, Anda harus memperbarui kebijakan berbasis sumber daya fungsi Anda untuk menghapus izin atau menambahkan kondisi. `AWS:SourceAccount` Anda hanya dapat memperbarui kebijakan berbasis sumber daya dari API Lambda atau. AWS CLI

Untuk memulai, tin jau kebijakan berbasis sumber daya di konsol Lambda. Mengidentifikasi pernyataan kebijakan yang memiliki nilai `Principal` bidang yang membuat kebijakan publik, seperti `"*"` atau`{ "AWS": "*" }`.

Anda tidak dapat mengedit kebijakan dari konsol. Untuk menghapus izin dari fungsi, jalankan remove-permission perintah dari AWS CLI.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

Ganti *`<function-name>`* dengan nama fungsi Lambda, dan *`<statement-id>`* dengan pernyataan ID (`Sid`) dari pernyataan yang ingin Anda hapus.

[Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/12.3.4

Kategori: Mel indungi > Pengembangan yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: lambda-function-settings-check

Jenis jadwal: Perubahan dipicu

Parameter:

- `runtime`: `dotnet10, dotnet8, java25, java21, java17, java11, java8.al2, java17.al2023, java11.al2023, java8.al2023, nodejs24.x, nodejs22.x, python3.14, python3.13, python3.12, python3.11, python3.10, ruby4.0, ruby3.4, ruby3.3` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pengaturan runtime AWS Lambda fungsi cocok dengan nilai yang diharapkan yang ditetapkan untuk runtime yang didukung di setiap bahasa. Kontrol gagal jika fungsi Lambda tidak menggunakan runtime yang didukung, seperti dicatat di bagian Parameter. Security Hub CSPM mengabaikan fungsi yang memiliki tipe paket. `Image`

Lambda runtime dibangun di sekitar kombinasi sistem operasi, bahasa pemrograman, dan pustaka perangkat lunak yang tunduk pada pemeliharaan dan pembaruan keamanan. Ketika komponen runtime tidak lagi didukung untuk pembaruan keamanan, Lambda menghentikan runtime. Meskipun Anda tidak dapat membuat fungsi yang menggunakan runtime yang tidak digunakan lagi, fungsi ini masih tersedia untuk memproses peristiwa pemanggilan. Sebaiknya pastikan fungsi Lambda Anda terkini dan tidak menggunakan lingkungan runtime yang tidak digunakan lagi. Untuk daftar runtime yang didukung, lihat runtime Lambda di Panduan Pengembang. AWS Lambda

Remediasi

Untuk informasi selengkapnya tentang runtime yang didukung dan jadwal penghentian, lihat Kebijakan penghentian Runtime di Panduan Pengembang. AWS Lambda Saat Anda memigrasikan runtime ke versi terbaru, ikuti sintaks dan panduan dari penerbit bahasa tersebut. Kami juga merekomendasikan menerapkan pembaruan runtime untuk membantu mengurangi risiko dampak pada beban kerja Anda jika terjadi ketidakcocokan versi runtime yang jarang terjadi.

[Lambda.3] Fungsi lambda harus dalam VPC

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: lambda-inside-vpc

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah fungsi Lambda digunakan di cloud pribadi virtual (VPC). Kontrol gagal jika fungsi Lambda tidak digunakan di VPC. Security Hub CSPM tidak mengevaluasi konfigurasi routing subnet VPC untuk menentukan jangkauan publik. Anda mungkin melihat temuan gagal untuk sumber daya Lambda @Edge.

Menyebarkan sumber daya dalam VPC memperkuat keamanan dan kontrol atas konfigurasi jaringan. Penerapan semacam itu juga menawarkan skalabilitas dan toleransi kesalahan yang tinggi di beberapa Zona Ketersediaan. Anda dapat menyesuaikan penerapan VPC untuk memenuhi persyaratan aplikasi yang beragam.

Remediasi

Untuk mengonfigurasi fungsi yang ada untuk menyambung ke subnet pribadi di VPC Anda, lihat Meng konfigurasi akses VPC di Panduan Peng AWS Lambda embang. Sebaiknya pilih setidaknya dua subnet pribadi untuk ketersediaan tinggi dan setidaknya satu grup keamanan yang memenuhi persyaratan konektivitas fungsi.

[Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: lambda-vpc-multi-az-check

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`availabilityZones`	Jumlah Zona Ketersediaan Minimum	Enum	`2, 3, 4, 5, 6`	2

Kontrol ini memeriksa apakah AWS Lambda fungsi yang terhubung ke cloud pribadi virtual (VPC) beroperasi setidaknya dalam jumlah Availability Zone (AZ) yang ditentukan. Kontrol gagal jika fungsi tidak beroperasi setidaknya dalam jumlah AZ yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk jumlah minimum AZ, Security Hub CSPM menggunakan nilai default dua AZ.

Menyebarkan sumber daya di beberapa AZ adalah praktik AWS terbaik untuk memastikan ketersediaan tinggi dalam arsitektur Anda. Ketersediaan adalah pilar inti dalam model keamanan triad kerahasiaan, integritas, dan ketersediaan. Semua fungsi Lambda yang terhubung ke VPC harus memiliki penerapan Multi-AZ untuk memastikan bahwa satu zona kegagalan tidak menyebabkan gangguan total operasi.

Remediasi

Jika Anda mengonfigurasi fungsi untuk terhubung ke VPC di akun Anda, tentukan subnet di beberapa AZ untuk memastikan ketersediaan tinggi. Untuk petunjuk, lihat Meng konfigurasi akses VPC di Panduan Peng AWS Lambda embang.

Lambda secara otomatis menjalankan fungsi lain di beberapa AZ untuk memastikan bahwa itu tersedia untuk memproses peristiwa jika terjadi gangguan layanan dalam satu zona.

[Lambda.6] Fungsi lambda harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: `tagged-lambda-function` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		AWS persyaratan.	

Kontrol ini memeriksa apakah suatu AWS Lambda fungsi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika fungsi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika fungsi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke fungsi Lambda, lihat Menggunakan tag pada fungsi Lambda di Panduan Peng AWS Lambda embang.

[Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-7

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Lambda::Function`

AWS Config aturan: lambda-function-xray-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pelacakan aktif dengan AWS X-Ray diaktifkan untuk suatu AWS Lambda fungsi. Kontrol gagal jika pelacakan aktif dengan dinon X-Ray aktifkan untuk fungsi Lambda.

AWS X-Ray dapat memberikan kemampuan pelacakan dan pemantauan untuk AWS Lambda fungsi, yang dapat menghemat waktu dan upaya debugging dan pengoperasian fungsi Lambda. Ini dapat membantu Anda mendiagnosis kesalahan dan mengidentifikasi hambatan kinerja, perlambatan, dan batas waktu dengan memecah latensi untuk fungsi Lambda. Ini juga dapat membantu dengan persyaratan privasi dan kepatuhan data. Jika Anda mengaktifkan pelacakan aktif untuk fungsi Lambda, X-Ray menyediakan tampilan holistik aliran data dan pemrosesan dalam fungsi Lambda, yang dapat membantu Anda mengidentifikasi potensi kerentanan keamanan atau praktik penanganan data yang tidak sesuai. Visibilitas ini dapat membantu Anda menjaga integritas data, kerahasiaan, dan kepatuhan terhadap peraturan yang relevan.

> **Note**
>
> AWS X-Ray pelacakan saat ini tidak didukung untuk fungsi Lambda dengan Amazon Managed Streaming untuk Apache Kafka (Amazon MSK), Apache Kafka yang dikelola sendiri, Amazon MQ dengan ActiveMQ dan RabbitMQ, atau pemetaan sumber peristiwa Amazon DocumentDB.

Remediasi

Untuk informasi tentang mengaktifkan pelacakan aktif untuk suatu AWS Lambda fungsi, lihat Visualisasikan pemanggilan fungsi Lambda menggunakan AWS X-Ray di Panduan Peng AWS Lambda embang.

Kontrol CSPM Security Hub untuk Macie

AWS Security Hub CSPMKontrol ini mengevaluasi layanan Amazon Macie.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Macie.1] Amazon Macie harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`macie-status-check`**

Jenis jadwal: Periodik

Kontrol ini memeriksa apakah Amazon Macie diaktifkan untuk sebuah akun. Kontrol gagal jika Macie tidak diaktifkan untuk akun.

Amazon Macie menemukan data sensitif menggunakan pembelajaran mesin dan pencocokan pola, memberikan visibilitas ke risiko keamanan data, dan memungkinkan perlindungan otomatis terhadap risiko tersebut. Macie secara otomatis dan terus-menerus mengevaluasi bucket Amazon Simple Storage Service (Amazon S3) Anda untuk keamanan dan kontrol akses, serta menghasilkan temuan untuk memberi tahu Anda tentang potensi masalah terkait keamanan atau privasi data Amazon S3 Anda. Macie juga mengotomatiskan penemuan dan pelaporan data sensitif, seperti informasi identitas pribadi (PII), untuk memberi Anda pemahaman yang lebih baik tentang data yang Anda simpan di Amazon S3. Untuk mempelajari lebih lanjut, lihat Panduan Pengguna Amazon Macie.

Remediasi

Untuk mengaktifkan Macie, lihat Mengaktifkan Macie di Panduan Pengguna Amazon Macie.

[Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: **`macie-auto-sensitive-data-discovery-check`**

Jenis jadwal: Periodik

Kontrol ini memeriksa apakah penemuan data sensitif otomatis diaktifkan untuk akun administrator Amazon Macie. Kontrol gagal jika penemuan data sensitif otomatis tidak diaktifkan untuk akun administrator Macie. Kontrol ini hanya berlaku untuk akun administrator.

Macie mengotomatiskan penemuan dan pelaporan data sensitif, seperti informasi identitas pribadi (PII), di bucket Amazon Simple Storage Service (Amazon S3). Dengan penemuan data sensitif otomatis, Macie terus mengevaluasi inventaris bucket Anda dan menggunakan teknik pengambilan sampel untuk mengidentifikasi dan memilih objek S3 yang representatif dari bucket Anda. Macie kemudian menganalisis objek yang dipilih, memeriksanya untuk data sensitif. Seiring kemajuan analisis, Macie memperbarui statistik, data inventaris, dan informasi lain yang diberikannya tentang data S3 Anda. Macie juga menghasilkan temuan untuk melaporkan data sensitif yang ditemukannya.

Remediasi

Untuk membuat dan mengonfigurasi tugas penemuan data sensitif otomatis untuk menganalisis objek di bucket S3, lihat Mengonfigurasi penemuan data sensitif otomatis untuk akun Anda di Panduan Pengguna Amazon Macie.

Kontrol CSPM Security Hub untuk Amazon MSK

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Managed Streaming for Apache Kafka (Amazon MSK). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Configaturan: msk-in-cluster-node-require-tls

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster MSK Amazon dienkripsi dalam perjalanan dengan HTTPS (TLS) di antara node broker cluster. Kontrol gagal jika komunikasi teks biasa diaktifkan untuk koneksi node broker cluster.

HTTPS menawarkan lapisan keamanan ekstra karena menggunakan TLS untuk memindahkan data dan dapat digunakan untuk membantu mencegah penyerang potensial menggunakan serangan person-in-the-middle atau serupa untuk menguping atau memanipulasi lalu lintas jaringan. Secara default, Amazon MSK mengenkripsi data dalam perjalanan dengan TLS. Namun, Anda dapat mengganti default ini pada saat Anda membuat cluster. Sebaiknya gunakan koneksi terenkripsi melalui HTTPS (TLS) untuk koneksi node broker.

Remediasi

Untuk informasi tentang memperbarui setelan enkripsi untuk klaster MSK Amazon, lihat Memperbarui setelan keamanan klaster di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

[MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Configaturan: msk-enhanced-monitoring-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster MSK Amazon telah meningkatkan pemantauan yang dikonfigurasi, yang ditentukan oleh tingkat pemantauan setidaknya`PER_TOPIC_PER_BROKER`. Kontrol gagal jika tingkat pemantauan untuk cluster diatur ke `DEFAULT` atau`PER_BROKER`.

Tingkat `PER_TOPIC_PER_BROKER` pemantauan memberikan wawasan yang lebih terperinci tentang kinerja klaster MSK Anda, dan juga menyediakan metrik yang terkait dengan pemanfaatan sumber

daya, seperti penggunaan CPU dan memori. Ini membantu Anda mengidentifikasi kemacetan kinerja dan pola pemanfaatan sumber daya untuk masing-masing topik dan broker. Visibilitas ini, pada gilirannya, dapat mengoptimalkan kinerja broker Kafka Anda.

Remediasi

Untuk mengonfigurasi pemantauan yang disempurnakan untuk klaster MSK, selesaikan langkah-langkah berikut:

1. Buka konsol MSK Amazon dihttps://console.aws.amazon.com/msk/home? region=us-east-1#/home/.
2. Pada panel navigasi, silakan pilih Klaster. Kemudian, pilih cluster.
3. Untuk Tindakan, pilih Edit pemantauan.
4. Pilih opsi untuk pemantauan tingkat topik yang ditingkatkan.
5. Pilih Simpan perubahan.

Untuk informasi selengkapnya tentang tingkat pemantauan, lihat metrik MSK Amazon untuk memantau pialang Standar CloudWatch di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

[MSK.3] Konektor MSK Connect harus dienkripsi saat transit

Persyaratan terkait: PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::KafkaConnect::Connector`

AWS Configaturan: `msk-connect-connector-encrypted` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah konektor Amazon MSK Connect dienkripsi saat transit. Kontrol ini gagal jika konektor tidak dienkripsi saat transit.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antar node di cluster Anda atau antara klaster Anda dan aplikasi Anda. Data dapat bergerak di internet

atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Anda dapat mengaktifkan enkripsi saat transit saat Anda membuat konektor MSK Connect. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat konektor. Untuk informasi selengkapnya, lihat Membuat konektor di Panduan Pengembang Amazon Managed Streaming for Apache Kafka Kafka.

[MSK.4] Kluster MSK harus menonaktifkan akses publik

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Configaturan: msk-cluster-public-access-disabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses publik dinonaktifkan untuk klaster MSK Amazon. Kontrol gagal jika akses publik diaktifkan untuk kluster MSK.

Secara default, klien dapat mengakses kluster MSK Amazon hanya jika mereka berada di VPC yang sama dengan cluster. Semua komunikasi antara klien Kafka dan kluster MSK bersifat pribadi secara default dan data streaming tidak melintasi internet. Namun, jika cluster MSK dikonfigurasi untuk memungkinkan akses publik, siapa pun di internet dapat membuat koneksi ke broker Apache Kafka yang berjalan di dalam cluster. Hal ini dapat menyebabkan masalah seperti akses tidak sah, pelanggaran data, atau eksploitasi kerentanan. Jika Anda membatasi akses ke klaster dengan mengharuskan tindakan otentikasi dan otorisasi, Anda dapat membantu melindungi informasi sensitif dan menjaga integritas sumber daya Anda.

Remediasi

Untuk informasi tentang mengelola akses publik ke klaster MSK Amazon, lihat Mengaktifkan akses publik ke klaster yang disediakan MSK di Panduan Pengembang Amazon Managed Streaming for Apache Kafka.

[MSK.5] Konektor MSK seharusnya mengaktifkan logging

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::KafkaConnect::Connector`

AWS Configaturan: msk-connect-connector-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk konektor MSK Amazon. Kontrol gagal jika logging dinonaktifkan untuk konektor MSK.

Konektor MSK Amazon mengintegrasikan sistem eksternal dan layanan Amazon dengan Apache Kafka dengan terus menyalin data streaming dari sumber data ke cluster Apache Kafka, atau terus menyalin data dari cluster ke dalam data sink. MSK Connect dapat menulis peristiwa log yang dapat membantu men-debug konektor. Saat membuat konektor, Anda dapat menentukan nol atau lebih dari tujuan log berikut: Amazon CloudWatch Log, Amazon S3, dan Amazon Data Firehose.

> **Note**
>
> Nilai konfigurasi sensitif dapat muncul di log konektor jika plugin tidak mendefinisikan nilai-nilai tersebut sebagai rahasia. Kafka Connect memperlakukan nilai konfigurasi yang tidak ditentukan sama dengan nilai plaintext lainnya.

Remediasi

Untuk mengaktifkan logging untuk konektor MSK Amazon yang ada, Anda harus membuat ulang konektor dengan konfigurasi logging yang sesuai. Untuk informasi tentang opsi konfigurasi, lihat Logging untuk MSK Connect di Panduan Pengembang Amazon Managed Streaming for Apache Kafka Kafka.

[MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::MSK::Cluster`

AWS Configaturan: msk-unrestricted-access-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses yang tidak diautentikasi diaktifkan untuk klaster MSK Amazon. Kontrol gagal jika akses yang tidak diautentikasi diaktifkan untuk kluster MSK.

Amazon MSK mendukung otentikasi klien dan mekanisme otorisasi untuk mengontrol akses ke cluster. Mekanisme ini memverifikasi identitas klien yang terhubung ke cluster dan menentukan tindakan mana yang dapat dilakukan klien. Kluster MSK dapat dikonfigurasi untuk memungkinkan akses yang tidak diautentikasi, yang memungkinkan setiap klien dengan konektivitas jaringan untuk mempublikasikan dan berlangganan topik Kafka tanpa memberikan kredensyal. Menjalankan klaster MSK tanpa memerlukan otentikasi melanggar prinsip hak istimewa paling sedikit dan dapat mengekspos cluster ke akses yang tidak sah. Ini dapat memungkinkan klien untuk mengakses, memodifikasi, atau menghapus data dalam topik Kafka, berpotensi mengakibatkan pelanggaran data, modifikasi data yang tidak sah, atau gangguan layanan. Sebaiknya aktifkan mekanisme otentikasi seperti autentikasi IAM SASL/SCRAM, atau TLS bersama untuk memastikan kontrol akses yang tepat dan menjaga kepatuhan keamanan.

Remediasi

Untuk informasi tentang mengubah setelan autentikasi untuk kluster MSK Amazon, lihat bagian berikut dari Panduan Pengembang Amazon Managed Streaming for Apache Kafka: Perbarui pengaturan keamanan klaster MSK Amazon serta Otentikasi dan otorisasi untuk Apache Kafka API.

Kontrol CSPM Security Hub untuk Amazon MQ

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon MQ. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch

Persyaratan terkait: NIST.800-53.r5 AU-2,, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-12 NIST.800-53.r5 SI-4, PCI DSS v4.0. 1/10.3.3

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Configaturan: **`mq-cloudwatch-audit-log-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah broker Amazon MQ ActiveMQ mengalirkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika broker tidak mengalirkan log audit ke CloudWatch Log.

Dengan menerbitkan log broker ActiveMQ CloudWatch ke Log, Anda dapat CloudWatch membuat alarm dan metrik yang meningkatkan visibilitas informasi terkait keamanan.

Remediasi

Untuk melakukan streaming log broker ActiveMQ CloudWatch ke Log, lihat Mengonfigurasi Amazon MQ untuk log ActiveMQ di Panduan Pengembang Amazon MQ.

[MQ.4] Broker Amazon MQ harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Configaturan: `tagged-amazonmq-broker` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratanAWS.	

Kontrol ini memeriksa apakah broker Amazon MQ memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika broker tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika broker tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke broker Amazon MQ, lihat Menandai sumber daya di Panduan Pengembang Amazon MQ.

[MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Configaturan: **`mq-active-deployment-mode`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah mode penerapan untuk broker Amazon MQ ActiveMQ diatur ke. active/standby Kontrol gagal jika broker instans tunggal (diaktifkan secara default) ditetapkan sebagai mode penerapan.

Active/standby penyebaran menyediakan ketersediaan tinggi untuk broker Amazon MQ ActiveMQ Anda di file. Wilayah AWS Mode active/standby penerapan mencakup dua instance broker di dua Availability Zone yang berbeda, dikonfigurasi dalam pasangan redundan. Pialang ini berkomunikasi secara serempak dengan aplikasi Anda, yang dapat mengurangi waktu henti dan kehilangan data jika terjadi kegagalan.

Remediasi

Untuk membuat broker ActiveMQ baru active/standby dengan mode penerapan, lihat Membuat dan mengonfigurasi broker ActiveMQ di Panduan Pengembang Amazon MQ. Untuk mode Deployment, pilih Active/standby broker. Anda tidak dapat mengubah mode penerapan untuk broker yang ada. Sebagai gantinya, Anda harus membuat broker baru dan menyalin pengaturan dari broker lama.

[MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::AmazonMQ::Broker`

AWS Configaturan: **`mq-rabbit-deployment-mode`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah mode penerapan untuk broker Amazon MQ RabbitMQ disetel ke penerapan cluster. Kontrol gagal jika broker instans tunggal (diaktifkan secara default) ditetapkan sebagai mode penerapan.

Penerapan cluster memberikan ketersediaan tinggi untuk broker Amazon MQ RabbitMQ Anda di file. Wilayah AWS Penyebaran cluster adalah pengelompokan logis dari tiga node broker RabbitMQ, masing-masing dengan volume Amazon Elastic Block Store (Amazon EBS) sendiri dan status bersama. Penyebaran cluster memastikan bahwa data direplikasi ke semua node di cluster, yang dapat mengurangi waktu henti dan hilangnya data jika terjadi kegagalan.

Remediasi

Untuk membuat broker RabbitMQ baru dengan mode penerapan cluster, lihat Membuat dan menghubungkan ke broker RabbitMQ di Panduan Pengembang Amazon MQ. Untuk mode Deployment, pilih Penerapan cluster. Anda tidak dapat mengubah mode penerapan untuk broker yang ada. Sebagai gantinya, Anda harus membuat broker baru dan menyalin pengaturan dari broker lama.

Kontrol CSPM Security Hub untuk Neptunus

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Neptunus.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: **`neptune-cluster-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus dienkripsi saat istirahat. Kontrol gagal jika cluster DB Neptunus tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya. Mengenkripsi kluster DB Neptunus Anda melindungi data dan metadata Anda dari akses yang tidak sah. Ini juga memenuhi persyaratan kepatuhan untuk enkripsi data-at-rest dari sistem file produksi.

Remediasi

Anda dapat mengaktifkan enkripsi saat istirahat saat Anda membuat cluster DB Neptunus. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat Mengenkripsi sumber daya Neptunus saat istirahat di Panduan Pengguna Neptunus.

[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 AU-7 (1), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (5), NIST.800-53.r5 SI-7(8), PCI DSS v4.0. 1/10.3.3

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: **`neptune-cluster-cloudwatch-log-export-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster DB Neptunus menerbitkan log audit ke Amazon Logs. CloudWatch Kontrol gagal jika kluster DB Neptunus tidak mempublikasikan log audit ke Log. CloudWatch `EnableCloudWatchLogsExport`harus diatur ke`Audit`.

Amazon Neptunus dan CloudWatch Amazon terintegrasi sehingga Anda dapat mengumpulkan dan menganalisis metrik kinerja. Neptunus secara otomatis mengirimkan metrik CloudWatch ke dan juga mendukung Alarm. CloudWatch Log audit sangat dapat disesuaikan. Saat Anda mengaudit database, setiap operasi pada data dapat dipantau dan dicatat ke jejak audit, termasuk informasi tentang cluster database mana yang diakses dan bagaimana caranya. Sebaiknya kirim log ini CloudWatch untuk membantu Anda memantau kluster DB Neptunus Anda.

Remediasi

Untuk memublikasikan log audit Neptunus CloudWatch ke Log, lihat Menerbitkan log Neptunus ke Log CloudWatch Amazon di Panduan Pengguna Neptunus. Di bagian Log ekspor, pilih Audit.

[Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`

AWS Configaturan: **`neptune-cluster-snapshot-public-prohibited`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot cluster DB manual Neptunus bersifat publik. Kontrol gagal jika snapshot cluster DB manual Neptunus bersifat publik.

Snapshot manual cluster Neptunus DB tidak boleh dipublikasikan kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak terenkripsi sebagai publik, snapshot tersedia untuk semua. Akun AWS Cuplikan publik dapat mengakibatkan eksposur data yang tidak diinginkan.

Remediasi

Untuk menghapus akses publik untuk snapshot kluster DB manual Neptunus, lihat Berbagi snapshot cluster DB di Panduan Pengguna Neptunus.

[Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: **`neptune-cluster-deletion-protection-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus mengaktifkan perlindungan penghapusan. Kontrol gagal jika cluster DB Neptunus tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan klaster menawarkan lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh pengguna yang tidak sah. Cluster DB Neptunus tidak dapat dihapus saat perlindungan penghapusan diaktifkan. Anda harus menonaktifkan perlindungan penghapusan terlebih dahulu sebelum permintaan penghapusan berhasil.

Remediasi

Untuk mengaktifkan perlindungan penghapusan klaster DB Neptunus yang ada, lihat Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon Aurora.

[Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis

Persyaratan terkait: NIST.800-53.r5 SI-12

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: **`neptune-cluster-backup-retention-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub	
`minimumBackupRetentionPeriod`	Periode retensi cadangan minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah cluster DB Neptunus telah mengaktifkan pencadangan otomatis, dan periode retensi cadangan lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika cadangan tidak diaktifkan untuk cluster DB Neptunus, atau jika periode retensi kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi cadangan, Security Hub CSPM menggunakan nilai default 7 hari.

Pencadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Dengan mengotomatiskan cadangan untuk cluster DB Neptunus Anda, Anda akan dapat memulihkan sistem Anda ke titik waktu tertentu dan meminimalkan waktu henti dan kehilangan data.

Remediasi

Untuk mengaktifkan pencadangan otomatis dan menetapkan periode retensi cadangan untuk kluster DB Neptunus Anda, lihat Mengaktifkan pencadangan otomatis di Panduan Pengguna Amazon RDS. Untuk periode retensi Backup, pilih nilai yang lebih besar dari atau sama dengan 7.

[Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (18)

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`

AWS Configaturan: **`neptune-cluster-snapshot-encrypted`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot cluster Neptunus DB dienkripsi saat istirahat. Kontrol gagal jika cluster DB Neptunus tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah mendapatkan akses ke sana. Data dalam snapshot cluster DB Neptunus harus dienkripsi saat istirahat untuk lapisan keamanan tambahan.

Remediasi

Anda tidak dapat mengenkripsi snapshot cluster Neptunus DB yang ada. Sebagai gantinya, Anda harus mengembalikan snapshot ke cluster DB baru dan mengaktifkan enkripsi pada cluster. Anda dapat membuat snapshot terenkripsi dari cluster terenkripsi. Untuk petunjuknya, lihat Memulihkan dari snapshot cluster DB dan Membuat snapshot cluster DB di Neptunus di Panduan Pengguna Neptunus.

[Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: **`neptune-cluster-iam-database-authentication`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus memiliki otentikasi database IAM diaktifkan. Kontrol gagal jika otentikasi database IAM tidak diaktifkan untuk cluster DB Neptunus.

Autentikasi database IAM untuk kluster database Amazon Neptunus menghilangkan kebutuhan untuk menyimpan kredensil pengguna dalam konfigurasi database karena otentikasi dikelola secara eksternal menggunakan IAM. Ketika autentikasi database IAM diaktifkan, setiap permintaan harus ditandatangani menggunakan AWS Signature Version 4.

Remediasi

Secara default, otentikasi database IAM dinonaktifkan saat Anda membuat cluster DB Neptunus. Untuk mengaktifkannya, lihat Mengaktifkan otentikasi database IAM di Neptunus di Panduan Pengguna Neptunus.

[Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: **`neptune-cluster-copy-tags-to-snapshot-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Neptunus dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat. Kontrol gagal jika cluster DB Neptunus tidak dikonfigurasi untuk menyalin tag ke snapshot.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus menandai snapshot dengan cara yang sama seperti cluster database Amazon RDS induknya.

Menyalin tag memastikan bahwa metadata untuk snapshot DB cocok dengan cluster database induk, dan kebijakan akses untuk snapshot DB juga cocok dengan instans DB induk.

Remediasi

Untuk menyalin tag ke snapshot untuk kluster DB Neptunus, lihat Menyalin tag di Neptunus di Panduan Pengguna Neptunus.

[Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Configaturan: **`neptune-cluster-multi-az-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kluster DB Amazon Neptunus memiliki instance baca-replika di beberapa Availability Zones (AZ). Kontrol gagal jika cluster digunakan hanya dalam satu AZ.

Jika AZ tidak tersedia dan selama peristiwa pemeliharaan rutin, replika baca berfungsi sebagai target failover untuk instance utama. Artinya, jika instans primer gagal, Neptune mempromosikan instans replika baca menjadi instans primer. Sebaliknya, jika cluster DB Anda tidak menyertakan instance read-replica, cluster DB Anda tetap tidak tersedia saat instance utama gagal hingga dibuat ulang. Re-creating contoh utama membutuhkan waktu jauh lebih lama daripada mempromosikan replika baca. Untuk memastikan ketersediaan tinggi, sebaiknya Anda membuat satu atau lebih instance read-replica yang memiliki kelas instans DB yang sama dengan instans utama dan berada di AZ yang berbeda dari instance utama.

Remediasi

Untuk menerapkan cluster DB Neptunus di beberapa AZ, lihat instans DB di cluster Read-replica DB Neptunus di Panduan Pengguna Neptunus.

Kontrol CSPM Security Hub untukAWS Network Firewall

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Network Firewall layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Configaturan: netfw-multi-az-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini mengevaluasi apakah firewall yang dikelola AWS Network Firewall digunakan di beberapa Availability Zones (AZ). Kontrol gagal jika firewall digunakan hanya dalam satu AZ.

AWSInfrastruktur global mencakup banyakWilayah AWS. AZ secara fisik terpisah, lokasi terisolasi di setiap Wilayah yang dihubungkan oleh latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan menerapkan firewall Network Firewall di beberapa AZ, Anda dapat menyeimbangkan dan mengalihkan lalu lintas di antara AZ, yang membantu Anda merancang solusi yang sangat tersedia.

Remediasi

Menyebarkan firewall Network Firewall di beberapa AZ

1. Buka konsol Amazon VPC di. https://console.aws.amazon.com/vpc/
2. Di panel navigasi, di bawah Network Firewall, pilih Firewall.
3. Pada halaman Firewall, pilih firewall yang ingin Anda edit.
4. Pada halaman detail firewall, pilih tab Detail Firewall.
5. Di bagian Kebijakan terkait dan VPC, pilih Edit

6. Untuk menambahkan AZ baru, pilih Add New Subnet. Pilih AZ dan subnet yang ingin Anda gunakan. Pastikan Anda memilih setidaknya dua AZ.
7. Pilih Simpan.

[NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9),, NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2 NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7),, NIST.800-53.r5 SC-7 (9) NIST.800-53.r5 CA-7, (8),, NIST.800-53.r5 SI-3 (20) NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.1.20, 3.13.1 NIST.800-171.r2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::LoggingConfiguration`

AWS Configaturan: netfw-logging-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk AWS Network Firewall firewall. Kontrol gagal jika logging tidak diaktifkan untuk setidaknya satu jenis log atau jika tujuan logging tidak ada.

Logging membantu Anda menjaga keandalan, ketersediaan, dan kinerja firewall Anda. Di Network Firewall, logging memberi Anda informasi rinci tentang lalu lintas jaringan, termasuk waktu mesin stateful menerima aliran paket, informasi rinci tentang aliran paket, dan tindakan aturan stateful yang diambil terhadap aliran paket.

Remediasi

Untuk mengaktifkan logging untuk firewall, lihat Memperbarui konfigurasi logging firewall di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait

Persyaratan terkait: NIST.800-53.r5 CA-9 (1),, NIST.800-171.r2 3.1.3 NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.1

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Configaturan: netfw-policy-rule-group-associated

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan Network Firewall memiliki grup aturan stateful atau stateless yang terkait. Kontrol gagal jika kelompok aturan stateless atau stateful tidak ditugaskan.

Kebijakan firewall menentukan cara firewall Anda memantau dan menangani lalu lintas di Amazon Virtual Private Cloud (Amazon VPC). Konfigurasi kelompok aturan stateless dan stateful membantu memfilter paket dan arus lalu lintas, dan mendefinisikan penanganan lalu lintas default.

Remediasi

Untuk menambahkan grup aturan ke kebijakan Network Firewall, lihat Memperbarui kebijakan firewall di Panduan AWS Network Firewall Pengembang. Untuk informasi tentang membuat dan mengelola grup aturan, lihat Grup aturan di AWS Network Firewall.

[NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Configaturan: netfw-policy-default-action-full-packets

Jenis jadwal: Perubahan dipicu

Parameter:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah tindakan stateless default untuk paket penuh untuk kebijakan Network Firewall adalah drop atau forward. Kontrol lolos jika `Drop` atau `Forward` dipilih, dan gagal jika `Pass` dipilih.

Kebijakan firewall menentukan bagaimana firewall Anda memantau dan menangani lalu lintas di Amazon VPC. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default untuk `Pass` dapat memungkinkan lalu lintas yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan firewall, lihat Memperbarui kebijakan firewall di Panduan AWS Network Firewall Pengembang. Untuk tindakan default Stateless, pilih Edit. Kemudian, pilih Jatuhkan atau Teruskan ke grup aturan stateful sebagai Tindakan.

[NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

Persyaratan terkait: NIST.800-53.r5 CA-9 (1),, NIST.800-171.r2 3.1.3 NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1.14, 3.13.1, NIST.800-171.r2 3.13.6 NIST.800-171.r2

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Configaturan: netfw-policy-default-action-fragment-packets

Jenis jadwal: Perubahan dipicu

Parameter:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah tindakan stateless default untuk paket terfragmentasi untuk kebijakan Network Firewall adalah drop atau forward. Kontrol lolos jika `Drop` atau `Forward` dipilih, dan gagal jika `Pass` dipilih.

Kebijakan firewall menentukan bagaimana firewall Anda memantau dan menangani lalu lintas di Amazon VPC. Anda mengonfigurasi grup aturan stateless dan stateful untuk memfilter paket dan arus lalu lintas. Default untuk `Pass` dapat memungkinkan lalu lintas yang tidak diinginkan.

Remediasi

Untuk mengubah kebijakan firewall, lihat Memperbarui kebijakan firewall di Panduan AWS Network Firewall Pengembang. Untuk tindakan default Stateless, pilih Edit. Kemudian, pilih Jatuhkan atau Teruskan ke grup aturan stateful sebagai Tindakan.

[NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong

Persyaratan terkait: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), (21), NIST.800-53.r5 SC-7 NIST.800-53.r5 SC-7 (5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14, 3.13.1, 3.13.6 NIST.800-171.r2 NIST.800-171.r2

Kategori: Lindungi > Konfigurasi Jaringan Aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::RuleGroup`

AWS Configaturan: netfw-stateless-rule-group-not-empty

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup aturan stateless AWS Network Firewall berisi aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan berisi aturan yang menentukan bagaimana firewall Anda memproses lalu lintas di VPC Anda. Grup aturan stateless kosong, ketika ada dalam kebijakan firewall, mungkin memberi kesan bahwa grup aturan akan memproses lalu lintas. Namun, ketika grup aturan stateless kosong, itu tidak memproses lalu lintas.

Remediasi

Untuk menambahkan aturan ke grup aturan Firewall Jaringan, lihat Memperbarui grup aturan stateful di Panduan AWS Network Firewall Pengembang. Pada halaman detail firewall, untuk grup aturan Stateless, pilih Edit untuk menambahkan aturan.

[NetworkFirewall.7] Firewall Firewall Jaringan harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Configaturan: `tagged-networkfirewall-firewall` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah AWS Network Firewall firewall memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika firewall tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika firewall tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke firewall Network Firewall, lihat Menandai AWS Network Firewall sumber daya di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::NetworkFirewall::FirewallPolicy`

AWS Configaturan: `tagged-networkfirewall-firewallpolicy` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratanAWS.	

Kontrol ini memeriksa apakah kebijakan AWS Network Firewall firewall memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika kebijakan firewall tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika kebijakan firewall tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke kebijakan Network Firewall, lihat Menandai AWS Network Firewall sumber daya di Panduan AWS Network Firewall Pengembang.

[NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Configaturan: netfw-deletion-protection-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Network Firewall firewall memiliki perlindungan penghapusan diaktifkan. Kontrol gagal jika perlindungan penghapusan tidak diaktifkan untuk firewall.

AWS Network Firewalladalah firewall jaringan stateful, dikelola dan layanan deteksi intrusi yang memungkinkan Anda untuk memeriksa dan memfilter lalu lintas ke, dari, atau antara Virtual Private Clouds (VPC) Anda. Pengaturan perlindungan penghapusan melindungi terhadap penghapusan firewall yang tidak disengaja.

Remediasi

Untuk mengaktifkan proteksi penghapusan pada firewall Network Firewall yang ada, lihat Memperbarui firewall di Panduan AWS Network Firewall Pengembang. Untuk Ubah perlindungan, pilih Aktifkan. Anda juga dapat mengaktifkan perlindungan penghapusan dengan menjalankan UpdateFirewallDeleteProtectionAPI dan menyetel bidang ke. `DeleteProtection` `true`

[NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2,, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Lindungi > Keamanan Jaringan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::NetworkFirewall::Firewall`

AWS Configaturan: netfw-subnet-change-protection-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah perlindungan perubahan subnet diaktifkan untuk AWS Network Firewall firewall. Kontrol gagal jika perlindungan perubahan subnet tidak diaktifkan untuk firewall.

AWS Network Firewalladalah firewall jaringan stateful yang dikelola dan layanan deteksi intrusi yang dapat Anda gunakan untuk memeriksa dan memfilter lalu lintas ke, dari, atau di antara Virtual Private Clouds (VPC) Anda. Jika Anda mengaktifkan perlindungan perubahan subnet untuk firewall Network Firewall, Anda dapat melindungi firewall terhadap perubahan yang tidak disengaja pada asosiasi subnet firewall.

Remediasi

Untuk informasi tentang mengaktifkan perlindungan perubahan subnet untuk firewall Network Firewall yang ada, lihat Memperbarui firewall di Panduan AWS Network Firewall Pengembang.

Kontrol CSPM Security Hub untuk Amazon Service OpenSearch

AWS Security Hub CSPMKontrol ini mengevaluasi OpenSearch layanan dan sumber daya Amazon OpenSearch Service (Service). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-encrypted-at-rest`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain memiliki konfigurasi enkripsi saat istirahat diaktifkan. Pemeriksaan gagal jika enkripsi saat istirahat tidak diaktifkan.

Untuk lapisan keamanan tambahan untuk data sensitif, Anda harus mengonfigurasi domain OpenSearch Layanan Anda untuk dienkripsi saat istirahat. Saat Anda mengonfigurasi enkripsi data saat istirahat, AWS KMS menyimpan dan mengelola kunci enkripsi Anda. Untuk melakukan enkripsi, AWS KMS gunakan algoritma Advanced Encryption Standard dengan kunci 256-bit ()AES-256.

Untuk mempelajari lebih lanjut tentang enkripsi OpenSearch Layanan saat istirahat, lihat Enkripsi data saat istirahat untuk OpenSearch Layanan Amazon di Panduan Pengembang OpenSearch Layanan Amazon.

Remediasi

Untuk mengaktifkan enkripsi saat istirahat untuk OpenSearch domain baru dan yang sudah ada, lihat Mengaktifkan enkripsi data saat istirahat di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21),, NIST.800-53.r5 AC-6 NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-in-vpc-only`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain berada dalam VPC. Itu tidak mengevaluasi konfigurasi perutean subnet VPC untuk menentukan akses publik.

Anda harus memastikan bahwa OpenSearch domain tidak dilampirkan ke subnet publik. Lihat Resource-based kebijakan di Panduan Pengembang OpenSearch Layanan Amazon. Anda juga harus memastikan bahwa VPC Anda dikonfigurasi sesuai dengan praktik terbaik yang disarankan. Lihat Praktik terbaik keamanan untuk VPC Anda di Panduan Pengguna Amazon VPC.

OpenSearch domain yang digunakan dalam VPC dapat berkomunikasi dengan sumber daya VPC melalui AWS jaringan pribadi, tanpa perlu melintasi internet publik. Konfigurasi ini meningkatkan postur keamanan dengan membatasi akses ke data dalam perjalanan. VPC menyediakan sejumlah kontrol jaringan untuk mengamankan akses ke OpenSearch domain, termasuk ACL jaringan dan grup keamanan. Security Hub merekomendasikan agar Anda memigrasikan OpenSearch domain publik ke VPC untuk memanfaatkan kontrol ini.

Remediasi

Jika Anda membuat domain dengan titik akhir publik, Anda tidak dapat menempatkannya di dalam VPC nanti. Sebagai gantinya, Anda harus membuat domain baru dan memigrasi data Anda. Begitu juga sebaliknya. Jika Anda membuat domain dalam VPC, domain tersebut tidak dapat memiliki titik akhir publik. Sebagai gantinya, Anda harus membuat domain lain atau menonaktifkan kontrol ini.

Untuk petunjuknya, lihat Meluncurkan domain OpenSearch Layanan Amazon Anda dalam VPC di Panduan Pengembang Layanan OpenSearch Amazon.

[Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

Persyaratan terkait: NIST.800-53.r5 AC-4 NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23,, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-node-to-node-encryption-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain memiliki enkripsi node-to-node yang diaktifkan. Kontrol ini gagal jika enkripsi node-to-node dinonaktifkan pada domain.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menguping atau memanipulasi lalu lintas jaringan menggunakan serangan person-in-the-middle atau serupa. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengaktifkan enkripsi node-to-node untuk OpenSearch domain memastikan bahwa komunikasi intra-cluster dienkripsi dalam perjalanan.

Mungkin ada penalti kinerja yang terkait dengan konfigurasi ini. Anda harus mengetahui dan menguji trade-off kinerja sebelum mengaktifkan opsi ini.

Remediasi

Untuk mengaktifkan enkripsi node-ke-simpul pada OpenSearch domain, lihat Mengaktifkan enkripsi node-ke-simpul di Panduan Pengembang Layanan Amazon. OpenSearch

[Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-logs-to-cloudwatch`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `logtype = 'error'`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah OpenSearch domain dikonfigurasi untuk mengirim log kesalahan ke CloudWatch Log. Kontrol ini gagal jika error logging ke tidak CloudWatch diaktifkan untuk domain.

Anda harus mengaktifkan log kesalahan untuk OpenSearch domain dan mengirim log tersebut ke CloudWatch Log untuk penyimpanan dan respons. Log kesalahan domain dapat membantu audit keamanan dan akses, dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk mengaktifkan penerbitan log, lihat Mengaktifkan penerbitan log (konsol) di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-audit-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `cloudWatchLogsLogGroupArnList`(tidak dapat disesuaikan) - Security Hub CSPM tidak mengisi parameter ini. Comma-separated daftar grup CloudWatch log Log yang harus dikonfigurasi untuk log audit.

Kontrol ini memeriksa apakah OpenSearch domain telah mengaktifkan pencatatan audit. Kontrol ini gagal jika OpenSearch domain tidak mengaktifkan pencatatan audit.

Log audit sangat dapat disesuaikan. Mereka memungkinkan Anda melacak aktivitas pengguna di OpenSearch klaster Anda, termasuk keberhasilan dan kegagalan otentikasi, permintaan, perubahan indeksOpenSearch, dan kueri penelusuran yang masuk.

Remediasi

Untuk petunjuk cara mengaktifkan log audit, lihat Mengaktifkan log audit di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-data-node-fault-tolerance`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain dikonfigurasi dengan setidaknya tiga node data dan `zoneAwarenessEnabled` adalah`true`. Kontrol ini gagal untuk OpenSearch domain jika `instanceCount` kurang dari 3 atau `zoneAwarenessEnabled` kurang`false`.

Untuk mencapai ketersediaan tinggi tingkat cluster dan toleransi kesalahan, OpenSearch domain harus memiliki setidaknya tiga node data. Menyebarkan OpenSearch domain dengan setidaknya tiga node data memastikan operasi cluster jika node gagal.

Remediasi

Untuk memodifikasi jumlah node data dalam OpenSearch domain

1. Masuk ke AWS konsol dan buka konsol OpenSearch Layanan Amazon di https://console.aws.amazon.com/aos/.
2. Di bawah Domain saya, pilih nama domain yang akan diedit, dan pilih Edit.
3. Di bawah Data node mengatur Jumlah node ke angka yang lebih besar dari`3`. Jika Anda menerapkan ke tiga Availability Zone, setel nomor ke kelipatan tiga untuk memastikan distribusi yang sama di seluruh Availability Zone.
4. Pilih Kirim.

[Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen Akses Aman > Tindakan API sensitif dibatasi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-access-control-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah OpenSearch domain memiliki kontrol akses berbutir halus yang diaktifkan. Kontrol gagal jika kontrol akses berbutir halus tidak diaktifkan. Fine-grained kontrol akses memerlukan `advanced-security-options` OpenSearch parameter `update-domain-config` yang akan diaktifkan.

Fine-grained kontrol akses menawarkan cara tambahan untuk mengontrol akses ke data Anda di Amazon OpenSearch Service.

Remediasi

Untuk mengaktifkan kontrol akses berbutir halus, lihat kontrol Fine-grained akses di OpenSearch Layanan Amazon di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

Persyaratan terkait: NIST.800-53.r5 AC-17 (2) NIST.800-53.r5 AC-4,, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3) NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23,, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-https-required`**

Jenis jadwal: Perubahan dipicu

Parameter:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah titik akhir domain OpenSearch Layanan Amazon dikonfigurasi untuk menggunakan kebijakan keamanan TLS terbaru. Kontrol gagal jika titik akhir OpenSearch domain tidak dikonfigurasi untuk menggunakan kebijakan terbaru yang didukung atau jika HTTPS tidak diaktifkan.

HTTPS (TLS) dapat digunakan untuk membantu mencegah penyerang potensial menggunakan serangan person-in-the-middle atau serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui HTTPS (TLS) yang diizinkan. Mengenkripsi data dalam perjalanan dapat memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS. TLS 1.2 menyediakan beberapa peningkatan keamanan dibandingkan versi TLS sebelumnya.

Remediasi

Untuk mengaktifkan enkripsi TLS, gunakan operasi UpdateDomainConfigAPI. Konfigurasikan DomainEndpointOptionsbidang untuk menentukan nilai untuk`TLSSecurityPolicy`. Untuk informasi selengkapnya, lihat Node-to-node enkripsi di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.9] OpenSearch domain harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: `tagged-opensearch-domain` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratanAWS.	

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika domain tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika domain tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke domain OpenSearch Layanan, lihat Bekerja dengan tag di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru

Persyaratan terkait: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-update-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon memiliki pembaruan perangkat lunak terbaru yang diinstal. Kontrol gagal jika pembaruan perangkat lunak tersedia tetapi tidak diinstal untuk domain.

OpenSearch Pembaruan perangkat lunak layanan menyediakan perbaikan, pembaruan, dan fitur platform terbaru yang tersedia untuk lingkungan. Tetap up-to-date dengan instalasi patch membantu menjaga keamanan dan ketersediaan domain. Jika tidak ada tindakan yang diambil pada pembaruan yang diperlukan, perangkat lunak layanan diperbarui secara otomatis (biasanya setelah 2 minggu). Kami merekomendasikan penjadwalan pembaruan selama waktu lalu lintas rendah ke domain untuk meminimalkan gangguan layanan.

Remediasi

Untuk menginstal pembaruan perangkat lunak untuk OpenSearch domain, lihat Memulai pembaruan di Panduan Pengembang OpenSearch Layanan Amazon.

[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::OpenSearch::Domain`

AWS Configaturan: **`opensearch-primary-node-fault-tolerance`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah domain OpenSearch Layanan Amazon dikonfigurasi dengan setidaknya tiga node utama khusus. Kontrol gagal jika domain memiliki kurang dari tiga node utama khusus.

OpenSearch Layanan menggunakan node primer khusus untuk meningkatkan stabilitas cluster. Node utama khusus melakukan tugas manajemen klaster, tetapi tidak menyimpan data atau menanggapi permintaan unggahan data. Kami menyarankan Anda menggunakan Multi-AZ dengan standby, yang menambahkan tiga node utama khusus untuk setiap domain produksi OpenSearch .

Remediasi

Untuk mengubah jumlah node utama untuk OpenSearch domain, lihat Membuat dan mengelola domain OpenSearch Layanan Amazon di Panduan Pengembang OpenSearch Layanan Amazon.

Kontrol CSPM Security Hub untukAWS Private CA

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Private Certificate Authority (AWS Private CA) layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ACMPCA::CertificateAuthority`

AWS Configaturan: **`acm-pca-root-ca-disabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Private CA memiliki otoritas sertifikat root (CA) yang dinonaktifkan. Kontrol gagal jika root CA diaktifkan.

DenganAWS Private CA, Anda dapat membuat hierarki CA yang mencakup CA root dan CA bawahan. Anda harus meminimalkan penggunaan CA root untuk tugas sehari-hari, terutama di lingkungan produksi. CA root hanya boleh digunakan untuk menerbitkan sertifikat untuk CA perantara. Hal ini memungkinkan CA akar disimpan dari bahaya sementara CA perantara melakukan tugas harian menerbitkan sertifikat entitas akhir.

Remediasi

Untuk menonaktifkan root CA, lihat Memperbarui status CA di Panduan AWS Private Certificate Authority Pengguna.

[PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::ACMPCA::CertificateAuthority`

AWS Configaturan: `acmpca-certificate-authority-tagged`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah otoritas sertifikat CA AWS Pribadi memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredKeyTags`. Kontrol gagal jika otoritas sertifikat tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredKeyTags`. Jika parameter `requiredKeyTags` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika otoritas sertifikat tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk mengetahui praktik terbaik penandaan lainnya, lihat Praktik dan strategi terbaik di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

Remediasi

Untuk menambahkan tag ke otoritas CA AWS Pribadi, lihat Menambahkan tag untuk CA pribadi Anda di Panduan AWS Private Certificate Authority Pengguna.

Kontrol CSPM Hub Keamanan untuk Amazon RDS

AWS Security Hub CSPM Kontrol ini mengevaluasi sumber daya Amazon Relational Database Service (Amazon RDS) dan Amazon RDS. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[RDS.1] Snapshot RDS harus bersifat pribadi

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config aturan: `rds-snapshots-public-prohibited`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot Amazon RDS bersifat publik. Kontrol gagal jika snapshot RDS bersifat publik. Kontrol ini mengevaluasi instans RDS, instans Aurora DB, instans Neptune DB, dan cluster Amazon DocumentDB.

Snapshot RDS digunakan untuk membuat cadangan data pada instans RDS Anda pada titik waktu tertentu. Mereka dapat digunakan untuk memulihkan status instans RDS sebelumnya.

Snapshot RDS tidak boleh bersifat publik kecuali dimaksudkan. Jika Anda membagikan snapshot manual yang tidak dienkripsi sebagai publik, ini membuat snapshot tersedia untuk semua Akun AWS. Hal ini dapat mengakibatkan paparan data instans RDS yang tidak diinginkan.

Perhatikan bahwa jika konfigurasi diubah untuk memungkinkan akses publik, AWS Config aturan mungkin tidak dapat mendeteksi perubahan hingga 12 jam. Sampai AWS Config aturan mendeteksi perubahan, pemeriksaan akan lolos meskipun konfigurasi melanggar aturan.

Untuk mempelajari selengkapnya tentang berbagi snapshot DB, lihat Berbagi snapshot DB di Panduan Pengguna Amazon RDS.

Remediasi

Untuk menghapus akses publik dari snapshot RDS, lihat Berbagi snapshot di Panduan Pengguna Amazon RDS. Untuk visibilitas snapshot DB, kami memilih Pri badi.

[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.2.3, Benchmark Yay AWS asan CIS v3.0. 0/2.3.3, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-instance-public-access-check`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS dapat diakses publik dengan mengevaluasi `PubliclyAccessible` bidang dalam item konfigurasi instans.

`PubliclyAccessible`Nilai dalam konfigurasi instance RDS menunjukkan apakah instance DB dapat diakses publik. Ketika instance DB dikonfigurasi dengan`PubliclyAccessible`, itu adalah Internet-facing instance dengan nama DNS yang dapat diselesaikan secara publik, yang diselesaikan ke alamat IP publik. Ketika instance DB tidak dapat diakses publik, itu adalah instance internal dengan nama DNS yang diselesaikan ke alamat IP pribadi.

Kecuali Anda ingin instans RDS Anda dapat diakses publik, instans RDS tidak boleh dikonfigurasi dengan `PubliclyAccessible` nilai. Melakukannya mungkin memungkinkan lalu lintas yang tidak perlu ke instance database Anda.

Remediasi

Untuk menghapus akses publik dari instans DB RDS, lihat Memo difikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk akses publik, pilih No.

[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.2.1, Benchmark Yay AWS asan CIS v3.0. 0/2.3.1, Benchmark Yay AWS asan CIS v1.4. 0/2.3.1, NIST.800-53.r5 CA-9 (1),

NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-storage-encrypted`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah enkripsi penyimpanan diaktifkan untuk instans Amazon RDS DB Anda.

Kontrol ini ditujukan untuk instans RDS DB. Namun, ini juga dapat menghasilkan temuan untuk instans Aurora DB, instans Neptune DB, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda dapat menekannya.

Untuk lapisan keamanan tambahan untuk data sensitif Anda di instans DB RDS, Anda harus mengonfigurasi instans DB RDS agar dienkripsi saat diam. Untuk mengenkripsi instans DB RDS dan snapshot saat diam, aktifkan opsi enkripsi untuk instans DB RDS Anda. Data yang dienkripsi saat diam mencakup penyimpanan yang mendasari untuk instans DB, pencadangan otomatisnya, replika baca, dan snapshot.

Instans DB terenkripsi RDS menggunakan algoritma AES-256 enkripsi standar terbuka untuk mengenkripsi data Anda di server yang menghosting instans DB RDS Anda. Setelah data Anda dienkripsi, Amazon RDS menangani otentikasi akses dan dekripsi data Anda secara transparan dengan dampak minimal pada kinerja. Anda tidak perlu memodifikasi aplikasi klien database Anda untuk menggunakan enkripsi.

Enkripsi Amazon RDS saat ini tersedia untuk semua mesin database dan jenis penyimpanan. Enkripsi Amazon RDS tersedia untuk sebagian besar kelas instans DB. Untuk mempelajari tentang kelas instance DB yang tidak mendukung enkripsi Amazon RDS, lihat Mengen kripsi sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk informasi tentang mengenkripsi instans DB di Amazon RDS, lihat Mengen kripsi sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat diam

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config aturan: `rds-snapshot-encrypted`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah snapshot RDS DB dienkripsi. Kontrol gagal jika snapshot RDS DB tidak dienkripsi.

Kontrol ini ditujukan untuk instans RDS DB. Namun, ini juga dapat menghasilkan temuan untuk snapshot instans Aurora DB, instans Neptune DB, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda dapat menekannya.

Mengenkripsi data saat diam mengurangi risiko bahwa pengguna yang tidak diautentikasi mendapatkan akses ke data yang disimpan di disk. Data dalam snapshot RDS harus dienkripsi saat diam untuk lapisan keamanan tambahan.

Remediasi

Untuk mengenkripsi snapshot RDS, lihat Mengen kripsi sumber daya Amazon RDS di Panduan Pengguna Amazon RDS. Saat Anda mengenkripsi instance RDS DB, data terenkripsi mencakup penyimpanan yang mendasarinya untuk instance, pencadangan otomatisnya, replika baca, dan snapshot.

Anda hanya dapat mengenkripsi instance RDS DB saat Anda membuatnya, bukan setelah instance DB dibuat. Namun, karena Anda dapat mengenkripsi salinan snapshot yang tidak dienkripsi, Anda dapat menambahkan enkripsi secara efektif ke instans DB yang tidak terenkripsi. Artinya, Anda dapat membuat snapshot instans DB, lalu membuat salinan terenkripsi dari snapshot tersebut. Anda kemudian dapat memulihkan instans DB dari snapshot terenkripsi untuk menghasilkan salinan terenkripsi dari instans DB asli.

[RDS.5] Instans RDS DB harus dikonfigurasi dengan beberapa Zona Ketersediaan

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.2.4, NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-multi-az-support`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ketersediaan tinggi diaktifkan untuk instans DB RDS Anda. Kontrol gagal jika instance DB RDS tidak dikonfigurasi dengan beberapa Availability Zones (AZ). Kontrol ini tidak berlaku untuk instans DB RDS yang merupakan bagian dari penerapan cluster Multi-AZ DB.

Mengonfigurasi instans Amazon RDS DB dengan AZ membantu memastikan ketersediaan data yang disimpan. Multi-AZ penerapan memungkinkan failover otomatis jika ada masalah dengan ketersediaan AZ dan selama pemeliharaan RDS reguler.

Remediasi

Untuk menerapkan instans DB Anda di beberapa AZ, M emodifikasi instance DB menjadi penerapan instans Multi-AZ DB di Panduan Pengguna Amazon RDS.

[RDS.6] Pemantauan yang ditingkatkan harus dikonfigurasi untuk instans DB RDS

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-enhanced-monitoring-enabled`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan	
`monitoringInterval`	Jumlah detik antara interval pengumpulan metrik pemantauan	Enum	`1`, `5`, `10`, `15`, `30`, `60`	Tidak ada nilai default	

Kontrol ini memeriksa apakah pemantauan yang disempurnakan diaktifkan untuk instans DB Amazon Relational Database Service (Amazon RDS). Kontrol gagal jika pemantauan yang disempurnakan tidak diaktifkan untuk instance. Jika Anda memberikan nilai kustom untuk `monitoringInterval` parameter, kontrol hanya akan lolos jika metrik pemantauan yang disempurnakan dikumpulkan untuk instance pada interval yang ditentukan.

Di Amazon RDS, Enhanced Monitoring memungkinkan respons yang lebih cepat terhadap perubahan kinerja pada infrastruktur yang mendasarinya. Perubahan kinerja ini dapat mengakibatkan kurangnya ketersediaan data. Pemantauan yang Ditingkatkan menyediakan metrik real-time dari sistem operasi tempat instans DB RDS Anda berjalan. Agen diinstal pada instance. Agen dapat memperoleh metrik lebih akurat daripada yang mungkin dari lapisan hypervisor.

Metrik Pemantauan Ditingkatkan berguna ketika Anda ingin melihat bagaimana proses atau thread yang berbeda pada instans DB menggunakan CPU. Untuk informasi selengkapnya, lihat Pem antauan yang Ditingkatkan di Panduan Pengguna Amazon RDS.

Remediasi

Untuk petunjuk terperinci tentang mengaktifkan Pemantauan yang Ditingkatkan untuk instans DB Anda, lihat Men yiapkan dan mengaktifkan Pemantauan yang Ditingkatkan di Panduan Pengguna Amazon RDS.

[RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Mel indungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-deletion-protection-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS DB mengaktifkan perlindungan penghapusan. Kontrol gagal jika cluster DB RDS tidak mengaktifkan perlindungan penghapusan.

Kontrol ini ditujukan untuk instans RDS DB. Namun, ini juga dapat menghasilkan temuan untuk instans Aurora DB, instans Neptune DB, dan cluster Amazon DocumentDB. Jika temuan ini tidak berguna, maka Anda dapat menekannya.

Mengaktifkan perlindungan penghapusan cluster adalah lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh entitas yang tidak sah.

Ketika perlindungan penghapusan diaktifkan, cluster RDS tidak dapat dihapus. Sebelum permintaan penghapusan dapat berhasil, perlindungan penghapusan harus dinonaktifkan.

Remediasi

Untuk mengaktifkan perlindungan penghapusan untuk cluster RDS DB, lihat Memodifikasi cluster DB menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon RDS. Untuk Per lindungan penghapusan, pilih Aktifkan perlindungan penghapusan.

[RDS.8] Instans DB RDS harus mengaktifkan perlindungan penghapusan

Persyaratan terkait: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Mel indungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-instance-deletion-protection-enabled`

Jenis jadwal: Perubahan dipicu

Parameter:

- `databaseEngines`: `mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah instans DB RDS Anda yang menggunakan salah satu mesin database terdaftar mengaktifkan perlindungan penghapusan. Kontrol gagal jika instans DB RDS tidak mengaktifkan perlindungan penghapusan.

Mengaktifkan perlindungan penghapusan instans adalah lapisan perlindungan tambahan terhadap penghapusan atau penghapusan database yang tidak disengaja oleh entitas yang tidak sah.

Sementara perlindungan penghapusan diaktifkan, instance DB RDS tidak dapat dihapus. Sebelum permintaan penghapusan dapat berhasil, perlindungan penghapusan harus dinonaktifkan.

Remediasi

Untuk mengaktifkan perlindungan penghapusan untuk instans DB RDS, lihat Memo difikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk Per lindungan penghapusan, pilih Aktifkan perlindungan penghapusan.

[RDS.9] Instans RDS DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-logging-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance Amazon RDS DB dikonfigurasi untuk menerbitkan log berikut ke Amazon CloudWatch Logs. Kontrol gagal jika instance tidak dikonfigurasi untuk menerbitkan log berikut ke CloudWatch Log:

- Oracle: Peringatan, Audit, Jejak, Pendengar
- PostgreSQL: Postgresql, Tingkatkan
- MySQL: Audit, Kesalahan, Umum, SlowQuery
- MariaDB: Audit, Kesalahan, Umum, SlowQuery
- SQL Server: Kesalahan, Agen
- Aurora-MySQL: Audit, Kesalahan, Umum, SlowQuery
- Aurora-PostgreSQL: Postgresql

Database RDS harus mengaktifkan log yang relevan. Logging database menyediakan catatan terperinci dari permintaan yang dibuat ke RDS. Log database dapat membantu audit keamanan dan akses dan dapat membantu mendiagnosis masalah ketersediaan.

Remediasi

Untuk informasi tentang menerbitkan log database RDS ke Log CloudWatch , lihat Men entukan log yang akan dipublikasikan ke CloudWatch Log di Panduan Pengguna Amazon RDS.

[RDS.10] Otentikasi IAM harus dikonfigurasi untuk instans RDS

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: L indungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-instance-iam-authentication-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance RDS DB mengaktifkan otentikasi database IAM. Kontrol gagal jika otentikasi IAM tidak dikonfigurasi untuk instans DB RDS. Kontrol ini hanya mengevaluasi

instance RDS dengan jenis mesin berikut:`mysql`,,`postgres`,`aurora`, `aurora-mysqlaurora-postgresql`, dan`mariadb`. Instans RDS juga harus berada di salah satu status berikut agar temuan dapat dihasilkan:`available`,, `backing-upstorage-optimization`, atau`storage-full`.

Otentikasi database IAM memungkinkan otentikasi ke instance database dengan token otentikasi alih-alih kata sandi. Lalu lintas jaringan ke dan dari database dienkripsi menggunakan SSL. Untuk informasi selengkapnya, lihat otentikasi database IAM di Panduan Pengguna Amazon Aurora.

Remediasi

Untuk mengaktifkan otentikasi database IAM pada instans DB RDS, lihat Mengaktifkan dan menonaktifkan otentikasi database IAM di Panduan Pengguna Amazon RDS.

[RDS.11] Instans RDS harus mengaktifkan cadangan otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Kategori: Puli hkan > Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `db-instance-backup-enabled`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan	
`backupRetentionMinimum`	Periode retensi cadangan minimum dalam hari	Bilangan Bulat	7 untuk 35	7	

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan	
`checkReadReplicas`	Memeriksa apakah instans DB RDS mengaktifkan cadangan untuk replika baca	Boolean	Tidak dapat disesuaikan	`false`	

Kontrol ini memeriksa apakah instance Layanan Database Relasional Amazon mengaktifkan pencadangan otomatis, dan periode retensi cadangan lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Replika baca dikecualikan dari evaluasi. Kontrol gagal jika pencadangan tidak diaktifkan untuk instans, atau jika periode retensi kurang dari jangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi cadangan, Security Hub CSPM menggunakan nilai default 7 hari.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan dan memperkuat ketahanan sistem Anda. Amazon RDS memungkinkan Anda mengonfigurasi snapshot volume instans penuh harian. Untuk informasi selengkapnya tentang pencadangan otomatis Amazon RDS, lihat Bekerja dengan Cadangan di Panduan Pengguna Amazon RDS.

Remediasi

Untuk mengaktifkan pencadangan otomatis pada instans DB RDS, lihat Mengaktifkan pencadangan otomatis di Panduan Pengguna Amazon RDS.

[RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Lindungi > Manajemen akses aman > Otentikasi tanpa kata sandi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-iam-authentication-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon RDS DB mengaktifkan otentikasi database IAM.

Otentikasi database IAM memungkinkan otentikasi bebas kata sandi ke instance database. Otentikasi menggunakan token otentikasi. Lalu lintas jaringan ke dan dari database dienkripsi menggunakan SSL. Untuk informasi selengkapnya, lihat otentikasi database IAM di Panduan Pengguna Amazon Aurora.

Remediasi

Untuk mengaktifkan otentikasi IAM untuk cluster DB, lihat Mengaktifkan dan menonaktifkan otentikasi basis data IAM di Panduan Pengguna Amazon Aurora.

[RDS.13] Upgrade versi minor otomatis RDS harus diaktifkan

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.2.2, Benchmark Yay AWS asan CIS v3.0. 0/2.3.2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Kategori: Identifikasi > Kerentanan, patch, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-automatic-minor-version-upgrade-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans Amazon RDS DB mengaktifkan peningkatan versi minor otomatis. Kontrol gagal jika peningkatan versi minor otomatis tidak diaktifkan untuk instans DB RDS.

> **Note**
>
> Kontrol ini mengevaluasi setiap instans Amazon RDS DB secara independen. Untuk cluster Amazon Aurora, peningkatan versi minor otomatis mengharuskan Anda mengaktifkan pengaturan ini di cluster. Anda juga harus mengaktifkan pengaturan ini pada semua instance

di cluster. Penem PASSED uan untuk instance individual tidak menjamin bahwa peningkatan terjadi jika Anda juga belum mengaktifkan setelan di tingkat cluster.
Kontrol ini juga tidak memperhitungkan konfigurasi yang tidak mendukung peningkatan versi minor otomatis. Ini termasuk cluster Aurora dalam database global Aurora dan cluster Aurora MySQL dengan replika baca lintas wilayah. Untuk konfigurasi ini, kontrol mungkin menghasilkan hasil evaluasi yang tidak secara akurat mencerminkan perilaku peningkatan aktual.

Upgrade versi minor otomatis secara berkala memperbarui database ke versi mesin database terbaru. Namun, upgrade mungkin tidak selalu menyertakan versi mesin database terbaru. Jika Anda perlu menyimpan database pada versi tertentu pada waktu-waktu tertentu, sebaiknya Anda memutakhirkan secara manual ke versi database yang Anda butuhkan sesuai dengan jadwal yang Anda butuhkan. Dalam kasus masalah keamanan kritis atau ketika versi mencapai tanggal akhir dukungan, Amazon RDS mungkin menerapkan peningkatan versi minor meskipun Anda belum mengaktifkan opsi peningkatan versi minor otomatis. Untuk informasi selengkapnya, lihat dokumentasi peningkatan Amazon RDS untuk mesin database spesifik Anda:

- Upgrade versi minor otomatis untuk RDS untuk MariaDB
- Upgrade versi minor otomatis untuk RDS untuk MySQL
- Upgrade versi minor otomatis untuk RDS untuk PostgreSQL
- Db2 pada versi Amazon RDS
- Peningkatan versi minor Oracle
- Peningkatan mesin Microsoft SQL Server DB

Remediasi

Untuk mengaktifkan peningkatan versi minor otomatis untuk instans DB yang ada, lihat Memo difikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk Upgrade versi minor otomatis, pilih Ya.

[RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5)

Kategori: Puli hkan > Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `aurora-mysql-backtracking-enabled`

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan	
`BacktrackWindowInHours`	Jumlah jam untuk melacak kembali cluster Aurora MySQL	Ganda	`0.1` untuk `72`	Tidak ada nilai default	

Kontrol ini memeriksa apakah cluster Amazon Aurora mengaktifkan backtracking. Kontrol gagal jika cluster tidak mengaktifkan backtracking. Jika Anda memberikan nilai kustom untuk `BacktrackWindowInHours` parameter, kontrol hanya akan lolos jika cluster dilacak mundur untuk jangka waktu yang ditentukan.

Cadangan membantu Anda memulihkan lebih cepat dari insiden keamanan. Mereka juga memperkuat ketahanan sistem Anda. Aurora backtracking mengurangi waktu untuk memulihkan database ke titik waktu tertentu. Itu tidak memerlukan pemulihan database untuk melakukannya.

Remediasi

Untuk mengaktifkan backtracking Aurora, lihat Mengon figurasi backtracking di Panduan Pengguna Amazon Aurora.

Perhatikan bahwa Anda tidak dapat mengaktifkan backtracking pada cluster yang ada. Sebagai gantinya, Anda dapat membuat klon yang mengaktifkan backtracking. Untuk informasi selengkapnya tentang batasan backtracking Aurora, lihat daftar batasan di Ikh tisar back tracking.

[RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.2.4, NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-multi-az-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ketersediaan tinggi diaktifkan untuk cluster DB RDS Anda. Kontrol gagal jika cluster DB RDS tidak digunakan di beberapa Availability Zones (AZ).

Cluster RDS DB harus dikonfigurasi untuk beberapa AZ untuk memastikan ketersediaan data yang disimpan. Penerapan ke beberapa AZ memungkinkan failover otomatis jika terjadi masalah ketersediaan AZ dan selama acara pemeliharaan RDS reguler.

Remediasi

Untuk menerapkan cluster DB Anda di beberapa AZ, Memo difikasi instance DB menjadi penerapan instans Multi-AZ DB di Panduan Pengguna Amazon RDS.

Langkah-langkah remediasi berbeda untuk database global Aurora. Untuk mengonfigurasi beberapa Zona Ketersediaan untuk database global Aurora, pilih cluster DB Anda. Kemudian, pilih T ind akan dan Tambahkan pembaca, dan tentukan beberapa AZ. Untuk informasi selengkapnya, lihat Men ambahkan Replika Aurora ke cluster DB di Panduan Pengguna Amazon Aurora.

[RDS.16] Cluster Aurora DB harus dikonfigurasi untuk menyalin tag ke snapshot DB

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-copy-tags-to-snapshots-enabled` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon Aurora DB dikonfigurasi untuk secara otomatis menyalin tag ke snapshot cluster DB saat snapshot dibuat. Kontrol gagal jika cluster Aurora DB tidak dikonfigurasi untuk secara otomatis menyalin tag ke snapshot cluster saat snapshot dibuat.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus memiliki visibilitas dari semua cluster Amazon Aurora DB Anda sehingga Anda dapat menilai postur keamanannya dan mengambil tindakan pada area kelemahan potensial. Snapshot Aurora DB harus memiliki tag yang sama dengan cluster DB induknya. Di Amazon Aurora, Anda dapat mengonfigurasi cluster DB untuk secara otomatis menyalin semua tag untuk cluster ke snapshot cluster. Mengaktifkan pengaturan ini memastikan bahwa snapshot DB mewarisi tag yang sama dengan cluster DB induknya.

Remediasi

Untuk informasi tentang mengonfigurasi cluster Amazon Aurora DB untuk menyalin tag secara otomatis ke snapshot DB, lihat M emodifikasi cluster Amazon Aurora DB di Panduan Pengguna Amazon Aurora.

[RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Kategori: Identifikasi > Inventaris

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-instance-copy-tags-to-snapshots-enabled` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance RDS DB dikonfigurasi untuk menyalin semua tag ke snapshot saat snapshot dibuat.

Identifikasi dan inventaris aset TI Anda adalah aspek penting dari tata kelola dan keamanan. Anda harus memiliki visibilitas dari semua instans DB RDS Anda sehingga Anda dapat menilai postur keamanannya dan mengambil tindakan pada area kelemahan potensial. Snapshot harus diberi tag

dengan cara yang sama seperti instance database RDS induknya. Mengaktifkan pengaturan ini memastikan bahwa snapshot mewarisi tag dari instance database induknya.

Remediasi

Untuk menyalin tag secara otomatis ke snapshot untuk instans DB RDS, lihat Memo difikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Pilih Salin tag ke snapshot.

[RDS.19] Langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa cluster kritis

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-cluster-event-notifications-configured` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan acara Amazon RDS yang ada untuk cluster database memiliki notifikasi yang diaktifkan untuk jenis sumber dan pasangan nilai kunci kategori peristiwa berikut ini:

```
DBCluster: ["maintenance","failure"]
```

Kontrol akan lolos jika tidak ada langganan acara yang ada di akun Anda.

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang notifikasi peristiwa RDS, lihat Menggunakan notifikasi peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi peristiwa cluster RDS, lihat Berlangganan pemberitahuan acara Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	klaster
Cluster untuk disertakan	Semua cluster
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.20] Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/11.5.2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-instance-event-notifications-configured` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah langganan acara Amazon RDS yang ada untuk instans database memiliki notifikasi yang diaktifkan untuk jenis sumber dan pasangan nilai kunci kategori peristiwa berikut:

```
DBInstance: ["maintenance","configuration change","failure"]
```

Kontrol akan lolos jika tidak ada langganan acara yang ada di akun Anda.

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons cepat. Untuk informasi tambahan tentang notifikasi peristiwa RDS, lihat Menggunakan notifikasi peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi peristiwa instans RDS, lihat Berlangganan pemberitahuan acara Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Contoh
Contoh untuk disertakan	Semua contoh
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.21] Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/11.5.2

Kategori: Deteksi > Layanan deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-pg-event-notifications-configured` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ada langganan acara Amazon RDS dengan pemberitahuan diaktifkan untuk jenis sumber berikut, pasangan kunci-nilai kategori peristiwa. Kontrol akan lolos jika tidak ada langganan acara yang ada di akun Anda.

```
DBParameterGroup: ["configuration change"]
```

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan

respons cepat. Untuk informasi tambahan tentang notifikasi peristiwa RDS, lihat Menggunakan notifikasi peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi peristiwa grup parameter database RDS, lihat Ber langganan pemberitahuan peristiwa Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Grup parameter
Grup parameter yang akan disertakan	Semua kelompok parameter
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.22] Langganan notifikasi peristiwa RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0. 1/11.5.2

Kategori: Deteksi > Layanan Deteksi > Pemantauan aplikasi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::EventSubscription`

AWS Config aturan: `rds-sg-event-notifications-configured` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ada langganan acara Amazon RDS dengan pemberitahuan diaktifkan untuk jenis sumber berikut, pasangan kunci-nilai kategori peristiwa. Kontrol akan lolos jika tidak ada langganan acara yang ada di akun Anda.

```
DBSecurityGroup: ["configuration change","failure"]
```

Pemberitahuan peristiwa RDS menggunakan Amazon SNS untuk membuat Anda mengetahui perubahan ketersediaan atau konfigurasi sumber daya RDS Anda. Pemberitahuan ini memungkinkan respons yang cepat. Untuk informasi tambahan tentang notifikasi peristiwa RDS, lihat Menggunakan notifikasi peristiwa Amazon RDS di Panduan Pengguna Amazon RDS.

Remediasi

Untuk berlangganan notifikasi peristiwa instans RDS, lihat Berlangganan pemberitahuan acara Amazon RDS di Panduan Pengguna Amazon RDS. Gunakan nilai berikut:

Bidang	Nilai
Jenis sumber	Grup keamanan
Grup keamanan untuk disertakan	Semua grup keamanan
Kategori acara untuk disertakan	Pilih kategori acara tertentu atau Semua kategori acara

[RDS.23] Instans RDS tidak boleh menggunakan port default mesin database

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-no-default-ports` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster atau instance RDS menggunakan port selain port default mesin database. Kontrol gagal jika cluster atau instance RDS menggunakan port default. Kontrol ini tidak berlaku untuk instans RDS yang merupakan bagian dari cluster.

Jika Anda menggunakan port yang diketahui untuk menyebarkan cluster atau instance RDS, penyerang dapat menebak informasi tentang cluster atau instance. Penyerang dapat menggunakan informasi ini bersama dengan informasi lain untuk terhubung ke cluster atau instance RDS atau mendapatkan informasi tambahan tentang aplikasi Anda.

Saat Anda mengubah port, Anda juga harus memperbarui string koneksi yang ada yang digunakan untuk terhubung ke port lama. Anda juga harus memeriksa grup keamanan instans DB untuk memastikan bahwa itu menyertakan aturan masuk yang memungkinkan konektivitas pada port baru.

Remediasi

Untuk mengubah port default instans DB RDS yang ada, lihat Memo difikasi instans Amazon RDS DB di Panduan Pengguna Amazon RDS. Untuk memodifikasi port default cluster RDS DB yang ada, lihat M emodifikasi cluster DB dengan menggunakan konsol, CLI, dan API di Panduan Pengguna Amazon Aurora. Untuk port Database, ubah nilai port menjadi nilai non-default.

[RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/2.2.2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-default-admin-check`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster database Amazon RDS telah mengubah nama pengguna admin dari nilai defaultnya. Kontrol tidak berlaku untuk mesin tipe Neptune (Neptune DB) atau docdb (DocumentDB). Aturan ini akan gagal jika nama pengguna admin disetel ke nilai default.

Saat membuat database Amazon RDS, Anda harus mengubah nama pengguna admin default menjadi nilai unik. Nama pengguna default adalah pengetahuan publik dan harus diubah selama pembuatan database RDS. Mengubah nama pengguna default mengurangi risiko akses yang tidak diinginkan.

Remediasi

Untuk mengubah nama pengguna admin yang terkait dengan cluster database Amazon RDS, buat cluster database RDS baru dan ubah nama pengguna admin default saat membuat database.

[RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, PCI DSS v4.0. 1/2.2.2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-instance-default-admin-check`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Anda telah mengubah nama pengguna administratif untuk instans database Amazon Relational Database Service (Amazon RDS) dari nilai default. Kontrol gagal jika nama pengguna administratif diatur ke nilai default. Kontrol tidak berlaku untuk mesin tipe Neptune (Neptune DB) atau docdb (DocumentDB), dan untuk instance RDS yang merupakan bagian dari cluster.

Nama pengguna administratif default di database Amazon RDS adalah pengetahuan publik. Saat membuat database Amazon RDS, Anda harus mengubah nama pengguna administratif default menjadi nilai unik untuk mengurangi risiko akses yang tidak diinginkan.

Remediasi

Untuk mengubah nama pengguna administratif yang terkait dengan instance database RDS, pertama buat instance database RDS baru. Ubah nama pengguna administratif default saat membuat database.

[RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan

Kategori: Puli hkan > Ketahanan > Cadangan diaktifkan

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `rds-resources-protected-by-backup-plan`

Jenis jadwal: Ber kala

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan	
`backupVaultLockCheck`	Kontrol menghasilkan tem `PASSED` uan jika parameter disetel ke true dan sumber daya menggunakan AWS Backup Vault Lock.	Boolean	`true` atau `false`	Tidak ada nilai default	

Kontrol ini mengevaluasi apakah instans Amazon RDS DB dicakup oleh rencana cadangan. Kontrol ini gagal jika instance RDS DB tidak tercakup oleh rencana cadangan. Jika Anda menetapkan `backupVaultLockCheck` parameter sama dengan`true`, kontrol hanya akan lolos jika instance dicadangkan dalam vault yang AWS Backup terkunci.

> **Note**
>
> Kontrol ini tidak mengevaluasi instans Neptunus dan DocumentDB. Itu juga tidak mengevaluasi instance RDS DB yang merupakan anggota cluster.

AWS Backup adalah layanan pencadangan yang dikelola sepenuhnya yang memusatkan dan mengotomatiskan pencadangan data di seluruh. Layanan AWS Dengan AWS Backup, Anda dapat

membuat kebijakan cadangan yang disebut rencana cadangan. Anda dapat menggunakan paket ini untuk menentukan persyaratan pencadangan, seperti seberapa sering membuat cadangan data Anda dan berapa lama untuk menyimpan cadangan tersebut. Menyertakan instans DB RDS dalam paket cadangan membantu Anda melindungi data dari kehilangan atau penghapusan yang tidak diinginkan.

Remediasi

Untuk menambahkan instance RDS DB ke paket AWS Backup cadangan, lihat Men etapkan sumber daya ke rencana cadangan di Panduan Peng AWS Backup embang.

[RDS.27] Cluster RDS DB harus dienkripsi saat diam

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-encrypted-at-rest`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster RDS DB dienkripsi saat diam. Kontrol gagal jika cluster DB RDS tidak dienkripsi saat diam.

Data diam mengacu pada data apa pun yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi apa pun. Enkripsi membantu Anda melindungi kerahasiaan data tersebut, mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya. Mengenkripsi cluster RDS DB melindungi data dan metadata Anda dari akses yang tidak sah. Ini juga memenuhi persyaratan kepatuhan untuk enkripsi data-at-rest sistem file produksi.

Remediasi

Anda dapat mengaktifkan enkripsi saat diam saat membuat cluster RDS DB. Anda tidak dapat mengubah pengaturan enkripsi setelah membuat cluster. Untuk informasi selengkapnya, lihat Mengenkripsi cluster Amazon Aurora DB di Panduan Pengguna Amazon Aurora.

[RDS.28] Cluster DB RDS harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `tagged-rds-dbcluster` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah cluster Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika cluster DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Menandai juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke cluster RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.29] Snapshot cluster RDS DB harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBClusterSnapshot`

AWS Config aturan: `tagged-rds-dbclustersnapshot` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
			AWS persyaratan.	

Kontrol ini memeriksa apakah snapshot cluster Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika snapshot cluster DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Menandai juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot cluster RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.30] Instans DB RDS harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: `tagged-rds-dbinstance` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah instance Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika instance DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika instance DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Menandai juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke instans DB RDS, lihat Men andai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.31] Grup keamanan RDS DB harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBSecurityGroup`

AWS Config aturan: `tagged-rds-dbsecuritygroup` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
			AWS persyaratan.	

Kontrol ini memeriksa apakah grup keamanan Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika grup keamanan DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup keamanan DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Menandai juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup keamanan RDS DB, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.32] Snapshot DB RDS harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBSnapshot`

AWS Config aturan: `tagged-rds-dbsnapshot` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah snapshot Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika snapshot DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Menandai juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan

kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot DB RDS, lihat Menandai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.33] Grup subnet RDS DB harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBSubnetGroup`

AWS Config aturan: `tagged-rds-dbsubnetgroups` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah grup subnet Amazon RDS DB memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet DB tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet DB tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Menandai juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan tagging, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau kumpulan kebijakan terpisah untuk kepala sekolah IAM Anda. Anda dapat merancang kebijakan ABAC ini untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag sumber daya. Untuk informasi selengkapnya, lihat Untuk apa ABAC? AWSdalam Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orang Layanan AWS, termasuk AWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Men andai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet RDS DB, lihat Men andai sumber daya Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-aurora-mysql-audit-logging-enabled`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Amazon Aurora MySQL dikonfigurasi untuk menerbitkan log audit ke Amazon CloudWatch Logs. Kontrol gagal jika cluster tidak dikonfigurasi untuk menerbitkan log audit ke CloudWatch Log. Kontrol tidak menghasilkan temuan untuk cluster Aurora Serverless v1 DB.

Log audit menangkap catatan aktivitas database, termasuk upaya login, modifikasi data, perubahan skema, dan peristiwa lain yang dapat diaudit untuk tujuan keamanan dan kepatuhan. Saat mengonfigurasi cluster Aurora MySQL DB untuk menerbitkan log audit ke grup log di Amazon CloudWatch Logs, Anda dapat melakukan analisis data log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Anda juga dapat membuat alarm dan melihat metrik di CloudWatch.

> **Note**
>
> Cara alternatif untuk mempublikasikan log audit ke Log CloudWatch adalah dengan mengaktifkan audit lanjutan dan menyetel parameter DB tingkat cluster ke. `server_audit_logs_upload` 1 Default untuk `server_audit_logs_upload` `parameter` adalah`0`. Namun, sebaiknya gunakan petunjuk remediasi berikut sebagai gantinya untuk melewati kontrol ini.

Remediasi

Untuk menerbitkan log audit cluster Aurora MySQL DB ke CloudWatch Log, lihat Menerbitkan log Amazon Aurora MySQL ke Amazon CloudWatch Log di Panduan Pengguna Amazon Aurora.

[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis

Persyaratan terkait: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5), PCI DSS v4.0. 1/6.3.3

Kategori: Identifikasi > Kerentanan, patch, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: `rds-cluster-auto-minor-version-upgrade-enable`

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah peningkatan versi minor otomatis diaktifkan untuk cluster Amazon RDS DB, termasuk cluster Aurora DB. Kontrol gagal jika peningkatan versi minor otomatis tidak diaktifkan untuk cluster DB.

Dengan peningkatan versi minor otomatis, Anda dapat memperbarui cluster DB Anda. Versi minor dapat memperkenalkan fitur perangkat lunak baru, perbaikan bug, patch keamanan, dan peningkatan kinerja. Dengan mengaktifkan peningkatan versi minor otomatis pada cluster database RDS, cluster, bersama dengan instans di cluster, akan menerima pembaruan otomatis ke versi minor ketika versi baru tersedia. Pembaruan diterapkan secara otomatis selama jendela pemeliharaan.

Remediasi

Untuk mengaktifkan peningkatan versi minor otomatis pada cluster Multi-AZ DB, lihat M emodifikasi cluster Multi-AZ DB di Panduan Pengguna Amazon RDS.

Untuk mengaktifkan peningkatan versi minor otomatis pada cluster Aurora DB, lihat M emodifikasi cluster Amazon Aurora DB di Panduan Pengguna Amazon Aurora.

[RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: rds-postgresql-logs-to-cloudwatch

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`logTypes`	Comma-separated daftar jenis log yang akan dipublikasikan ke CloudWatch Log	StringList	Tidak dapat disesuaikan	`postgresql`

Kontrol ini memeriksa apakah instans DB Amazon RDS untuk PostgreSQL dikonfigurasi untuk menerbitkan log ke Amazon Logs. CloudWatch Kontrol gagal jika instance PostgreSQL DB tidak dikonfigurasi untuk menerbitkan jenis log yang disebutkan dalam `logTypes` parameter ke CloudWatch Log.

Logging database menyediakan catatan terperinci dari permintaan yang dibuat ke instance RDS. PostgreSQL menghasilkan log peristiwa yang berisi informasi berguna untuk administrator. Menerbitkan log ini ke CloudWatch Log memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Anda juga dapat membuat alarm dan melihat metrik diCloudWatch.

Remediasi

Untuk menerbitkan log instans DB PostgreSQL ke Log, lihat Mener bitkan CloudWatch log PostgreSQL ke CloudWatch Log Amazon di Panduan Pengguna Amazon RDS.

[RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: rds-aurora-postgresql-logs-to-cloudwatch

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster DB Amazon Aurora PostgreSQL dikonfigurasi untuk menerbitkan log ke Amazon CloudWatch Logs. Kontrol gagal jika cluster DB Aurora PostgreSQL tidak dikonfigurasi untuk menerbitkan log PostgreSQL ke Log. CloudWatch

Logging database menyediakan catatan terperinci dari permintaan yang dibuat ke cluster RDS. Aurora PostgreSQL menghasilkan log peristiwa yang berisi informasi berguna untuk administrator. Menerbitkan log ini ke CloudWatch Log memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Anda juga dapat membuat alarm dan melihat metrik di CloudWatch.

Remediasi

Untuk menerbitkan log cluster Aurora PostgreSQL DB ke Log, lihat Mener bitkan CloudWatch log Aurora PostgreSQL ke Amazon CloudWatch Log di Panduan Pengguna Amazon RDS.

[RDS.38] RDS untuk instans DB PostgreSQL harus dienkripsi saat transit

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: rds-postgres-instance-encrypted-in-transit

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke instance Amazon RDS for PostgreSQL database (DB) dienkripsi saat transit. Kontrol gagal jika `rds.force_ssl` parameter untuk grup parameter yang terkait dengan instance disetel ke `0` (off). Kontrol ini tidak mengevaluasi instans DB RDS yang merupakan bagian dari cluster DB.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antara node di cluster Anda atau antara cluster Anda dan aplikasi Anda. Data dapat bergerak melintasi internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Untuk mewajibkan semua koneksi ke instans DB RDS for PostgreSQL agar menggunakan SSL, lihat Menggunakan SSL dengan instans DB PostgreSQL di Panduan Pengguna Amazon RDS.

[RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: rds-mysql-instance-encrypted-in-transit

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke instance Amazon RDS for MySQL database (DB) dienkripsi saat transit. Kontrol gagal jika `rds.require_secure_transport` parameter untuk grup parameter yang terkait dengan instance disetel ke `0` (off). Kontrol ini tidak mengevaluasi instans DB RDS yang merupakan bagian dari cluster DB.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antara node di cluster Anda atau antara cluster Anda dan aplikasi Anda. Data dapat bergerak melintasi internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko bahwa pengguna yang tidak sah dapat menguping lalu lintas jaringan.

Remediasi

Untuk mewajibkan semua koneksi ke instans DB RDS for MySQL agar menggunakan SSL, lihat SSL/TLS dukungan untuk instans MySQL DB di Amazon RDS di Panduan Pengguna Amazon RDS.

[RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: rds-sql-server-logs-to-cloudwatch

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`logTypes`	Daftar jenis log yang RDS untuk instance SQL Server DB harus dikonfigurasi untuk dipublikasikan ke CloudWatch Log. Kontrol ini gagal jika instance DB tidak dikonfigurasi untuk menerbitkan jenis log yang ditentukan dalam daftar.	EnumList (maksimal 2 item)	`agent`, `error`	`agent`, `error`

Kontrol ini memeriksa apakah instans Amazon RDS untuk Microsoft SQL Server DB dikonfigurasi untuk menerbitkan log ke Amazon Log CloudWatch . Kontrol gagal jika instance RDS untuk SQL Server DB tidak dikonfigurasi untuk menerbitkan CloudWatch log ke Log. Anda dapat secara opsional menentukan jenis log yang instans DB harus dikonfigurasi untuk dipublikasikan.

Pencatatan database menyediakan catatan terperinci dari permintaan yang dibuat ke instans Amazon RDS DB. Menerbitkan CloudWatch log ke Log memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. CloudWatch Log menyimpan log dalam penyimpanan yang sangat tahan lama. Selain itu, Anda dapat menggunakannya untuk membuat alarm untuk kesalahan tertentu yang dapat terjadi, seperti sering restart yang dicatat dalam log kesalahan. Demikian pula, Anda dapat membuat alarm untuk kesalahan atau peringatan yang dicatat dalam log agen SQL Server terkait dengan pekerjaan agen SQL.

Remediasi

Untuk informasi tentang menerbitkan CloudWatch log ke Log untuk instance RDS untuk SQL Server DB, lihat file log database Amazon RDS untuk Microsoft SQL Server di Panduan Pengguna Layanan Database Relasional Amazon.

[RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: rds-sqlserver-encrypted-in-transit

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke instans DB Amazon RDS untuk Microsoft SQL Server dienkripsi saat transit. Kontrol gagal jika parameter grup `rds.force_ssl` parameter yang terkait dengan instance DB disetel ke`0 (off)`.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antara node dalam cluster DB atau antara cluster DB dan aplikasi klien. Data dapat bergerak melintasi internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko pengguna yang tidak sah menguping lalu lintas jaringan.

Remediasi

Untuk informasi tentang mengaktifkan SSL/TLS koneksi ke instans Amazon RDS DB yang menjalankan Microsoft SQL Server, lihat Menggunakan SSL dengan Instans DB Microsoft SQL Server di Panduan Pengguna Layanan Database Relasional Amazon.

[RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: mariadb-publish-logs-to-cloudwatch-logs

Jenis jadwal: Ber kala

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`logTypes`	Daftar jenis log yang instans MariaDB DB harus dikonfigu rasi untuk dipublikasikan ke CloudWatch Log. Kontrol menghasilkan tem `FAILED` uan jika instance DB tidak dikonfigurasi untuk menerbitk an jenis log yang ditentukan dalam daftar.	EnumList (maksimal 4 item)	`audit`, `error`, `general`, `slowquery`	`audit`, `error`

Kontrol ini memeriksa apakah instans Amazon RDS untuk MariaDB DB dikonfigurasi untuk menerbitkan jenis log tertentu ke Amazon Logs. CloudWatch Kontrol gagal jika instance MariaDB DB tidak dikonfigurasi untuk menerbitkan log ke CloudWatch Log. Anda dapat secara opsional menentukan jenis log mana yang harus dikonfigurasi instans MariaDB DB untuk dipublikasikan.

Pencatatan database menyediakan catatan terperinci dari permintaan yang dibuat ke instans DB Amazon RDS untuk MariaDB. Menerbitkan log ke Amazon CloudWatch Logs memusatkan manajemen log dan membantu Anda melakukan analisis data log secara real-time. Selain itu, CloudWatch Log menyimpan log dalam penyimpanan tahan lama, yang dapat mendukung tinjauan dan audit keamanan, akses, dan ketersediaan. Dengan CloudWatch Log, Anda juga dapat membuat alarm dan meninjau metrik.

Remediasi

Untuk informasi tentang mengonfigurasi instans Amazon RDS untuk MariaDB DB untuk menerbitkan log ke Amazon Logs, lihat Mener bitkan CloudWatch log MariaDB ke Amazon Log di Panduan Pengguna CloudWatch Layanan Database Rel asional Amazon.

[RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBProxy`

AWS Config aturan: rds-proxy-tls-encryption

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah proxy Amazon RDS DB memerlukan TLS untuk semua koneksi antara proxy dan instans DB RDS yang mendasarinya. Kontrol gagal jika proxy tidak memerlukan TLS untuk semua koneksi antara proxy dan instance RDS DB.

Amazon RDS Proxy dapat bertindak sebagai lapisan keamanan tambahan antara aplikasi klien dan instans RDS DB yang mendasarinya. Misalnya, Anda dapat menyambung ke proxy RDS menggunakan TLS 1.3, bahkan jika instance DB yang mendasarinya mendukung versi TLS yang lebih lama. Dengan menggunakan RDS Proxy, Anda dapat menerapkan persyaratan otentikasi yang kuat untuk aplikasi database.

Remediasi

Untuk informasi tentang mengubah pengaturan untuk proxy Amazon RDS agar memerlukan TLS, lihat Memo difikasi proxy RDS di Panduan Pengguna Layanan Database Relasional Amazon.

[RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: rds-mariadb-instance-encrypted-in-transit

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke instans DB Amazon RDS untuk MariaDB dienkripsi saat transit. Kontrol gagal jika grup parameter DB yang terkait dengan instance DB tidak sinkron, atau `require_secure_transport` parameter grup parameter tidak disetel ke`ON`.

> **Note**
>
> Kontrol ini tidak mengevaluasi instans Amazon RDS DB yang menggunakan versi MariaDB lebih awal dari versi 10.5. `require_secure_transport`Parameter ini didukung hanya untuk MariaDB versi 10.5 dan yang lebih baru.

Data dalam transit mengacu pada data yang berpindah dari satu lokasi ke lokasi lain, seperti antara node dalam cluster DB atau antara cluster DB dan aplikasi klien. Data dapat bergerak melintasi internet atau dalam jaringan pribadi. Mengenkripsi data dalam perjalanan mengurangi risiko pengguna yang tidak sah menguping lalu lintas jaringan.

Remediasi

Untuk informasi tentang mengaktifkan SSL/TLS koneksi ke instans Amazon RDS untuk MariaDB DB, lihat Membutuhkan semua koneksi ke instans MariaDB DB di Panduan Pengguna Layanan Database Relasional Amazon. SSL/TLS

[RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: aurora-mysql-cluster-audit-logging

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon Aurora MySQL DB mengaktifkan pencatatan audit. Kontrol gagal jika grup parameter DB yang terkait dengan cluster DB tidak sinkron, `server_audit_logging` parameter tidak disetel ke1, atau `server_audit_events` parameter disetel ke nilai kosong.

Log database dapat membantu audit keamanan dan akses serta membantu mendiagnosis masalah ketersediaan. Log audit menangkap catatan aktivitas database, termasuk upaya login, modifikasi data, perubahan skema, dan peristiwa lain yang dapat diaudit untuk tujuan keamanan dan kepatuhan.

Remediasi

Untuk informasi tentang mengaktifkan logging untuk cluster DB Amazon Aurora MySQL, lihat M enerbitkan log Amazon Aurora MySQL ke Amazon CloudWatch Log di Panduan Pengguna Amazon Aurora.

[RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RDS::DBInstance`

AWS Config aturan: rds-instance-subnet-igw-check

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance Amazon RDS DB digunakan di subnet publik yang memiliki rute ke gateway internet. Kontrol gagal jika instance RDS DB digunakan di subnet yang memiliki rute ke gateway internet dan tujuan disetel ke `0.0.0.0/0` atau. `::/0`

Dengan menyediakan sumber daya Amazon RDS di subnet pribadi, Anda dapat mencegah sumber daya RDS menerima lalu lintas masuk dari internet publik, yang dapat mencegah akses yang tidak diinginkan ke instans DB RDS Anda. Jika sumber daya RDS disediakan di subnet publik yang terbuka untuk internet, mereka mungkin rentan terhadap risiko seperti eksfiltrasi data.

Remediasi

Untuk informasi tentang penyediaan subnet pribadi untuk instans Amazon RDS DB, lihat Bek erja dengan instans DB di VPC di Panduan Pengguna Layanan Database Relasional Amazon.

[RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: rds-pgsql-cluster-copy-tags-to-snapshot-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon RDS untuk PostgreSQL DB dikonfigurasi untuk secara otomatis menyalin tag ke snapshot cluster DB saat snapshot dibuat. Kontrol gagal jika `CopyTagsToSnapshot` parameter disetel ke `false` untuk cluster DB RDS untuk PostgreSQL.

Menyalin tag ke snapshot DB membantu menjaga pelacakan sumber daya, tata kelola, dan alokasi biaya yang tepat di seluruh sumber daya cadangan. Hal ini memungkinkan identifikasi sumber daya yang konsisten, kontrol akses, dan pemantauan kepatuhan di kedua database aktif dan snapshot-nya. Snapshot yang diberi tag dengan benar meningkatkan operasi keamanan dengan memastikan sumber daya cadangan mewarisi metadata yang sama dengan basis data sumbernya.

Remediasi

Untuk informasi tentang mengonfigurasi cluster DB Amazon RDS for PostgreSQL untuk menyalin tag secara otomatis ke snapshot DB, lihat Men andai sumber daya Amazon RDS di Panduan Pengguna Layanan Database Relasional Amazon.

[RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: rds-mysql-cluster-copy-tags-to-snapshot-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon RDS for MySQL DB dikonfigurasi untuk secara otomatis menyalin tag ke snapshot cluster DB saat snapshot dibuat. Kontrol gagal jika `CopyTagsToSnapshot` parameter diatur `false` untuk cluster RDS untuk MySQL DB.

Menyalin tag ke snapshot DB membantu menjaga pelacakan sumber daya, tata kelola, dan alokasi biaya yang tepat di seluruh sumber daya cadangan. Hal ini memungkinkan identifikasi sumber daya yang konsisten, kontrol akses, dan pemantauan kepatuhan di kedua database aktif dan snapshot-nya. Snapshot yang diberi tag dengan benar meningkatkan operasi keamanan dengan memastikan sumber daya cadangan mewarisi metadata yang sama dengan basis data sumbernya.

Remediasi

Untuk informasi tentang mengonfigurasi cluster Amazon RDS for MySQL DB untuk menyalin tag secara otomatis ke snapshot DB, lihat Men andai sumber daya Amazon RDS di Panduan Pengguna Layanan Database Relasional Amazon.

[RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan

Kategori: Puli hkan > Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RDS::DBCluster`

AWS Config aturan: rds-cluster-backup-retention-check

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan	
`minimumBackupRetentionPeriod`	Periode retensi cadangan minimum dalam hari untuk diperiksa kontrol	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah cluster RDS DB memiliki periode retensi cadangan minimum. Kontrol gagal jika periode retensi cadangan kurang dari nilai parameter yang ditentukan. Kecuali Anda memberikan nilai parameter khusus, Security Hub menggunakan nilai default 7 hari.

Kontrol ini memeriksa apakah cluster RDS DB memiliki periode retensi cadangan minimum. Kontrol gagal jika periode retensi cadangan kurang dari nilai parameter yang ditentukan. Kecuali Anda memberikan nilai parameter pelanggan, Security Hub menggunakan nilai default 7 hari. Kontrol ini berlaku untuk semua jenis cluster DB RDS termasuk cluster Aurora DB, cluster DocumentDB, cluster NeptuneDB, dll.

Remediasi

Untuk mengonfigurasi periode retensi cadangan untuk cluster RDS DB, ubah pengaturan cluster dan atur periode retensi cadangan menjadi minimal 7 hari (atau nilai yang ditentukan dalam parameter kontrol). Untuk petunjuk terperinci, lihat Periode retensi cadangan di Panduan Pengguna Layanan Database Relasional Amazon. Untuk cluster Aurora DB, lihat Ringkasan tentang membuat cadangan dan memulihkan cluster Aurora DB di Panduan Pengguna Amazon Aurora untuk Aurora. Untuk jenis cluster DB lainnya (misalnya cluster DocumentDB), lihat panduan pengguna layanan terkait untuk cara memperbarui periode retensi cadangan untuk cluster.

[RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung

Kategori: Identifikasi > Kerentanan, patch, dan manajemen versi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RDS::GlobalCluster`

AWS Config aturan: rds-global-cluster-aurora-mysql-supported-version

Jenis jadwal: Perubahan dipicu

Parameter:

- `minSupportedEngineVersion`: `8.0.mysql_aurora.3.08.0` (tidak dapat disesuaikan)
- `longTermSupportVersion`: `8.0.mysql_aurora.3.04.0, 8.0.mysql_aurora.3.04.1, 8.0.mysql_aurora.3.04.2, 8.0.mysql_aurora.3.04.3` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah cluster global Amazon Aurora MySQL berjalan pada versi mesin minimum yang didukung. Kontrol gagal jika versi mesin cluster global Aurora MySQL berada di bawah versi minimum yang didukung dan tidak tercantum dalam parameter versi dukungan jangka panjang.

Menjalankan database global Aurora MySQL pada versi engine yang didukung membantu memastikan bahwa Anda memiliki akses ke patch keamanan terbaru, perbaikan bug, dan

peningkatan kinerja. Versi minor Aurora MySQL telah menentukan tanggal akhir dukungan standar, setelah itu mereka tidak lagi menerima patch penting. Menjalankan versi yang tidak didukung dapat mengekspos database global Anda ke kerentanan keamanan dan dapat mengakibatkan biaya Dukungan Diperpanjang Amazon RDS. Karena Aurora MySQL mengikuti siklus hidup dukungan yang tidak bersebelahan di mana versi dukungan jangka panjang (LTS) tetap didukung lebih lama daripada versi non-LTS berikutnya, kontrol ini juga memeriksa versi LTS yang masih di bawah dukungan standar. Untuk informasi selengkapnya, lihat Kalender rilis untuk Amazon Aurora MySQL di Catatan Rilis Amazon Aurora untuk Aurora MySQL.

Remediasi

Untuk informasi tentang memutakhirkan database global Aurora MySQL ke versi engine yang didukung, lihat Meng upgrade database global Amazon Aurora dan Meng upgrade Aurora MySQL dengan memodifikasi versi mesin di Panduan Pengguna Amazon Aurora.

Kontrol CSPM Security Hub untuk Amazon Redshift

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Redshift. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Redshift.1] Cluster Amazon Redshift harus melarang akses publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-cluster-public-access-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift dapat diakses publik. Ini mengevaluasi `PubliclyAccessible` bidang dalam item konfigurasi cluster.

`PubliclyAccessible`Atribut konfigurasi klaster Amazon Redshift menunjukkan apakah klaster dapat diakses publik. Ketika cluster dikonfigurasi dengan `PubliclyAccessible` set to`true`, itu adalah Internet-facing instance yang memiliki nama DNS yang dapat diselesaikan secara publik, yang diselesaikan ke alamat IP publik.

Ketika cluster tidak dapat diakses publik, itu adalah instance internal dengan nama DNS yang menyelesaikan ke alamat IP pribadi. Kecuali jika Anda bermaksud agar cluster Anda dapat diakses oleh publik, cluster tidak boleh dikonfigurasi dengan `PubliclyAccessible` set to`true`.

Remediasi

Untuk memperbarui klaster Amazon Redshift untuk menonaktifkan akses publik, lihat Memodifikasi klaster di Panduan Manajemen Pergeseran Merah Amazon. Setel Dapat diakses publik ke No.

[Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Configaturan: redshift-require-tls-ssl

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke kluster Amazon Redshift diperlukan untuk menggunakan enkripsi dalam perjalanan. Pemeriksaan gagal jika parameter cluster Amazon Redshift `require_SSL` tidak disetel ke. `True`

TLS dapat digunakan untuk membantu mencegah penyerang potensial menggunakan serangan person-in-the-middle atau serupa untuk menguping atau memanipulasi lalu lintas jaringan. Hanya koneksi terenkripsi melalui TLS yang diizinkan. Mengenkripsi data dalam perjalanan dapat

memengaruhi kinerja. Anda harus menguji aplikasi Anda dengan fitur ini untuk memahami profil kinerja dan dampak TLS.

Remediasi

Untuk memperbarui grup parameter Amazon Redshift agar memerlukan enkripsi, lihat Memodifikasi grup parameter di Panduan Manajemen Pergeseran Merah Amazon. Setel `require_ssl` ke Benar.

[Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis

Persyaratan terkait: NIST.800-53.r5 CP-10 NIST.800-53.r5 CP-6,, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-13 (5)

Kategori: Pulih> Ketahanan > Cadangan diaktifkan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-backup-enabled

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub	
`MinRetentionPeriod`	Periode retensi snapshot minimum dalam beberapa hari	Bilangan Bulat	7 untuk 35	7	

Kontrol ini memeriksa apakah klaster Amazon Redshift mengaktifkan snapshot otomatis, dan periode retensi yang lebih besar dari atau sama dengan kerangka waktu yang ditentukan. Kontrol gagal jika snapshot otomatis tidak diaktifkan untuk cluster, atau jika periode retensi kurang dari kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode retensi snapshot, Security Hub CSPM menggunakan nilai default 7 hari.

Cadangan membantu Anda pulih lebih cepat dari insiden keamanan. Mereka memperkuat ketahanan sistem Anda. Amazon Redshift mengambil snapshot periodik secara default. Kontrol ini memeriksa apakah snapshot otomatis diaktifkan dan dipertahankan setidaknya selama tujuh hari. Untuk detail selengkapnya tentang snapshot otomatis Amazon Redshift, lihat Snapshot otomatis di Panduan Manajemen Pergeseran Merah Amazon.

Remediasi

Untuk memperbarui periode retensi snapshot untuk klaster Amazon Redshift, lihat Memodifikasi klaster di Panduan Manajemen Pergeseran Merah Amazon. Untuk Backup, atur retensi Snapshot ke nilai 7 atau lebih tinggi.

[Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: `redshift-cluster-audit-logging-enabled` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift mengaktifkan pencatatan audit.

Pencatatan audit Amazon Redshift memberikan informasi tambahan tentang koneksi dan aktivitas pengguna di klaster Anda. Data ini dapat disimpan dan diamankan di Amazon S3 dan dapat membantu dalam audit dan investigasi keamanan. Untuk informasi selengkapnya, lihat Pencatatan audit database di Panduan Manajemen Pergeseran Merah Amazon.

Remediasi

Untuk mengonfigurasi pencatatan audit untuk klaster Amazon Redshift, lihat Mengonfigurasi audit menggunakan konsol di Panduan Manajemen Amazon Redshift.

[Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama

Persyaratan terkait: NIST.800-53.r5 CA-9 (1) NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9,, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Kategori: Identifikasi > Kerentanan, tambalan, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-cluster-maintenancesettings-check

Jenis jadwal: Perubahan dipicu

Parameter:

- `allowVersionUpgrade = true`(tidak dapat disesuaikan)

Kontrol ini memeriksa apakah pemutakhiran versi utama otomatis diaktifkan untuk klaster Amazon Redshift.

Mengaktifkan pemutakhiran versi utama otomatis memastikan bahwa pembaruan versi utama terbaru ke kluster Amazon Redshift diinstal selama jendela pemeliharaan. Pembaruan ini mungkin termasuk patch keamanan dan perbaikan bug. Tetap up to date dengan instalasi patch adalah langkah penting dalam mengamankan sistem.

Remediasi

Untuk mengatasi masalah ini dariAWS CLI, gunakan perintah Amazon `modify-cluster` Redshift, dan setel `--allow-version-upgrade` atribut. *`clustername`*adalah nama cluster Amazon Redshift Anda.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan

Persyaratan terkait: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Akses pribadi API

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-enhanced-vpc-routing-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah `EnhancedVpcRouting` diaktifkan.

Perutean VPC yang disempurnakan memaksa semua `COPY` dan `UNLOAD` lalu lintas antara cluster dan repositori data untuk melewati VPC Anda. Anda kemudian dapat menggunakan fitur VPC seperti grup keamanan dan daftar kontrol akses jaringan untuk mengamankan lalu lintas jaringan. Anda juga dapat menggunakan VPC Flow Logs untuk memantau lalu lintas jaringan.

Remediasi

Untuk petunjuk remediasi terperinci, lihat Mengaktifkan perutean VPC yang disempurnakan di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Identifikasi > Konfigurasi Sumber Daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-default-admin-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah klaster Amazon Redshift telah mengubah nama pengguna admin dari nilai defaultnya. Kontrol ini akan gagal jika nama pengguna admin untuk cluster Redshift disetel ke. `awsuser`

Saat membuat klaster Redshift, Anda harus mengubah nama pengguna admin default menjadi nilai unik. Nama pengguna default adalah pengetahuan publik dan harus diubah pada konfigurasi. Mengubah nama pengguna default mengurangi risiko akses yang tidak diinginkan.

Remediasi

Anda tidak dapat mengubah nama pengguna admin untuk klaster Amazon Redshift Anda setelah membuatnya. Untuk membuat klaster baru dengan nama pengguna non-default, lihat Langkah 1: Membuat contoh klaster Amazon Redshift di Panduan Memulai Amazon Redshift.

[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-cluster-kms-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah cluster Amazon Redshift dienkripsi saat istirahat. Kontrol gagal jika klaster Redshift tidak dienkripsi saat istirahat atau jika kunci enkripsi berbeda dari kunci yang disediakan dalam parameter aturan.

Di Amazon Redshift, Anda dapat mengaktifkan enkripsi database untuk cluster Anda untuk membantu melindungi data saat istirahat. Saat Anda mengaktifkan enkripsi untuk cluster, blok data dan metadata sistem dienkripsi untuk cluster dan snapshot-nya. Enkripsi data saat istirahat adalah praktik terbaik yang disarankan karena menambahkan lapisan manajemen akses ke data Anda. Mengenkripsi cluster Redshift saat istirahat mengurangi risiko bahwa pengguna yang tidak sah dapat mengakses data yang disimpan pada disk.

Remediasi

Untuk memodifikasi klaster Redshift agar menggunakan enkripsi KMS, lihat Mengubah enkripsi klaster di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.11] Cluster Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: `tagged-redshift-cluster` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke klaster Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::EventSubscription`

AWS Configaturan: `tagged-redshift-eventsubscription` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi	`No default value`

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
	yang dievaluasi. Kunci tag peka huruf besar dan kecil.		persyaratanAWS.	

Kontrol ini memeriksa apakah snapshot klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke langganan notifikasi peristiwa Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.13] Snapshot klaster Redshift harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterSnapshot`

AWS Configaturan: `tagged-redshift-clustersnapshot` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah snapshot klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika snapshot cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika snapshot cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian

kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke snapshot klaster Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.14] Grup subnet cluster Redshift harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterSubnetGroup`

AWS Configaturan: `tagged-redshift-clustersubnetgroup` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah grup subnet klaster Amazon Redshift memiliki tag dengan kunci spesifik yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika grup subnet cluster tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup subnet cluster tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke grup subnet klaster Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi

Persyaratan terkait: PCI DSS v4.0. 1/1.3.1

Kategori: Lindungi > Konfigurasi jaringan aman > Konfigurasi grup keamanan

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-unrestricted-port-access

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup keamanan yang terkait dengan cluster Amazon Redshift memiliki aturan masuk yang mengizinkan akses ke port cluster dari internet (0.0.0. 0/0 atau: :/0). Kontrol gagal jika aturan masuknya grup keamanan mengizinkan akses ke port cluster dari internet.

Mengizinkan akses masuk yang tidak terbatas ke port cluster Redshift (alamat IP dengan akhiran /0) dapat mengakibatkan akses atau insiden keamanan yang tidak sah. Kami merekomendasikan untuk menerapkan prinsip akses hak istimewa paling rendah saat membuat grup keamanan dan mengonfigurasi aturan masuk.

Remediasi

Untuk membatasi masuknya port klaster Redshift ke asal terbatas, lihat Bekerja dengan aturan grup keamanan di Panduan Pengguna Amazon VPC. Perbarui aturan di mana rentang port cocok dengan port cluster Redshift dan rentang port IP adalah 0.0.0. 0/0.

[Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::ClusterSubnetGroup`

AWS Configaturan: redshift-cluster-subnet-group-multi-az

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol memeriksa apakah grup subnet klaster Amazon Redshift memiliki subnet dari lebih dari satu Availability Zone (AZ). Kontrol gagal jika grup subnet cluster tidak memiliki subnet dari setidaknya dua AZ yang berbeda.

Mengkonfigurasi subnet di beberapa AZ membantu memastikan bahwa gudang data Redshift Anda dapat terus beroperasi bahkan ketika peristiwa kegagalan terjadi.

Remediasi

Untuk mengubah grup subnet klaster Redshift untuk menjangkau beberapa AZ, lihat Memodifikasi grup subnet cluster di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.17] Grup parameter cluster Redshift harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Redshift::ClusterParameterGroup`

AWS Configaturan: redshift-cluster-parameter-group-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah grup parameter cluster Amazon Redshift memiliki kunci tag yang ditentukan oleh parameter. `requiredKeyTags` Kontrol gagal jika grup parameter tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika grup parameter tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu

Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke grup parameter klaster Amazon Redshift, lihat Menandai sumber daya di Amazon Redshift di Panduan Manajemen Pergeseran Merah Amazon.

[Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ

Kategori: Pulihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Redshift::Cluster`

AWS Configaturan: redshift-cluster-multi-az-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah beberapa penerapan Availability Zones (Multi-AZ) diaktifkan untuk klaster Amazon Redshift. Kontrol gagal jika Multi-AZ penerapan tidak diaktifkan untuk klaster Amazon Redshift.

Amazon Redshift mendukung beberapa penerapan Availability Zones (Multi-AZ) untuk kluster yang disediakan. Jika Multi-AZ penerapan diaktifkan untuk klaster, gudang data Amazon Redshift dapat terus beroperasi dalam skenario kegagalan saat peristiwa tak terduga terjadi di Availability Zone (AZ). Multi-AZ Penerapan menyebarkan sumber daya komputasi di lebih dari satu AZ dan sumber daya

komputasi ini dapat diakses melalui satu titik akhir. Jika terjadi kegagalan AZ secara keseluruhan, sumber daya komputasi yang tersisa di AZ lain tersedia untuk melanjutkan pemrosesan beban kerja. Anda dapat mengonversi gudang Single-AZ data yang ada menjadi gudang Multi-AZ data. Sumber daya komputasi tambahan kemudian disediakan dalam AZ kedua.

Remediasi

Untuk informasi tentang mengonfigurasi Multi-AZ penerapan untuk klaster Amazon Redshift, lihat Mengonversi gudang data ke gudang Single-AZ data Multi-AZ di Panduan Manajemen Amazon Redshift.

Kontrol CSPM Security Hub untuk Amazon Redshift Serverless

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Redshift Serverless. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan

Kategori: Lindungi > Konfigurasi jaringan aman> Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RedshiftServerless::Workgroup`

AWS Configaturan: redshift-serverless-workgroup-routes-within-vpc

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah perutean VPC yang disempurnakan diaktifkan untuk grup kerja Amazon Redshift Tanpa Server. Kontrol gagal jika perutean VPC yang ditingkatkan dinonaktifkan untuk grup kerja.

Jika perutean VPC yang disempurnakan dinonaktifkan untuk workgroup Amazon Redshift Tanpa Server, Amazon Redshift merutekan lalu lintas melalui internet, termasuk lalu lintas ke layanan lain dalam jaringan. AWS Jika Anda mengaktifkan perutean VPC yang disempurnakan untuk grup kerja, Amazon Redshift memaksa semua `UNLOAD` lalu lintas antara cluster `COPY` dan repositori data Anda melalui virtual private cloud (VPC) berdasarkan layanan Amazon VPC. Dengan perutean VPC yang

disempurnakan, Anda dapat menggunakan fitur VPC standar untuk mengontrol aliran data antara cluster Amazon Redshift dan sumber daya lainnya. Ini termasuk fitur seperti grup keamanan VPC dan kebijakan titik akhir, daftar kontrol akses jaringan (ACL), dan server Domain Name System (DNS). Anda juga dapat menggunakan log aliran VPC untuk memantau `COPY` dan `UNLOAD` lalu lintas.

Remediasi

Untuk informasi selengkapnya tentang perutean VPC yang disempurnakan dan cara mengaktifkannya untuk grup kerja, lihat Mengontrol lalu lintas jaringan dengan perutean VPC yang disempurnakan Redshift di Panduan Manajemen Amazon Redshift.

[RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RedshiftServerless::Workgroup`

AWS Configaturan: redshift-serverless-workgroup-encrypted-in-transit

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah koneksi ke workgroup Amazon Redshift Tanpa Server diperlukan untuk mengenkripsi data dalam perjalanan. Kontrol gagal jika parameter `require_ssl` konfigurasi untuk workgroup diatur ke`false`.

Workgroup Amazon Redshift Tanpa Server adalah kumpulan sumber daya komputasi yang mengelompokkan sumber daya komputasi seperti RPU, grup subnet VPC, dan grup keamanan. Properti workgroup mencakup pengaturan jaringan dan keamanan. Pengaturan ini menentukan apakah koneksi ke workgroup harus diperlukan untuk menggunakan SSL untuk mengenkripsi data dalam perjalanan.

Remediasi

Untuk informasi tentang memperbarui setelan grup kerja Amazon Redshift Tanpa Server agar memerlukan koneksi SSL, lihat Menyambungkan ke Amazon Redshift Tanpa Server di Panduan Manajemen Amazon Redshift.

[RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::RedshiftServerless::Workgroup`

AWS Configaturan: redshift-serverless-workgroup-no-public-access

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses publik dinonaktifkan untuk grup kerja Amazon Redshift Tanpa Server. Ini mengevaluasi `publiclyAccessible` properti grup kerja Redshift Serverless. Kontrol gagal jika akses publik diaktifkan (`true`) untuk workgroup.

Pengaturan public access (`publiclyAccessible`) untuk workgroup Amazon Redshift Serverless menentukan apakah workgroup dapat diakses dari jaringan publik. Jika akses publik diaktifkan (`true`) untuk grup kerja, Amazon Redshift akan membuat alamat IP Elastis yang membuat grup kerja dapat diakses publik dari luar VPC. Jika Anda tidak ingin grup kerja dapat diakses publik, nonaktifkan akses publik untuk itu.

Remediasi

Untuk informasi tentang mengubah setelan akses publik untuk grup kerja Amazon Redshift Tanpa Server, lihat Melihat properti untuk grup kerja di Panduan Manajemen Amazon Redshift.

[RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys

Persyaratan terkait: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RedshiftServerless::Namespace`

AWS Configaturan: redshift-serverless-namespace-cmk-encryption

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`kmsKeyArns`	Daftar Nama Sumber Daya Amazon (ARN) AWS KMS keys untuk disertakan dalam evaluasi. Kontrol menghasilkan `FAILED` temuan jika namespace Redshift Tanpa Server tidak dienkripsi dengan kunci KMS dalam daftar.	StringList (maksimal 3 item)	1—3 ARN kunci KMS yang ada. Sebagai contoh: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` .	Tidak ada nilai default

Kontrol ini memeriksa apakah namespace Amazon Redshift Tanpa Server dienkripsi saat istirahat dengan pelanggan yang dikelola. AWS KMS key Kontrol gagal jika namespace Redshift Tanpa Server tidak dienkripsi dengan kunci KMS yang dikelola pelanggan. Anda dapat secara opsional menentukan daftar kunci KMS untuk kontrol untuk disertakan dalam evaluasi.

Di Amazon Redshift Tanpa Server, namespace mendefinisikan wadah logis untuk objek database. Kontrol ini secara berkala memeriksa apakah pengaturan enkripsi untuk namespace menentukan pelanggan yang dikelolaAWS KMS key, bukan kunci KMS yang AWS dikelola, untuk enkripsi data di namespace. Dengan kunci KMS yang dikelola pelanggan, Anda memiliki kendali penuh atas kunci tersebut. Ini termasuk mendefinisikan dan memelihara kebijakan kunci, mengelola hibah, memutar materi kriptografi, menetapkan tag, membuat alias, dan mengaktifkan dan menonaktifkan kunci.

Remediasi

Untuk informasi tentang memperbarui setelan enkripsi untuk namespace Amazon Redshift Tanpa Server dan menentukan pelanggan yang dikelolaAWS KMS key, lihat Mengubah AWS KMS key namespace di Panduan Manajemen Amazon Redshift.

[RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default

Kategori: Identifikasi > Konfigurasi sumber daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RedshiftServerless::Namespace`

AWS Configaturan: redshift-serverless-default-admin-check

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah nama pengguna admin untuk namespace Amazon Redshift Tanpa Server adalah nama pengguna admin default. `admin` Kontrol gagal jika nama pengguna admin untuk namespace Redshift Tanpa Server. `admin`

Saat membuat namespace Amazon Redshift Tanpa Server, Anda harus menentukan nama pengguna admin khusus untuk namespace. Nama pengguna admin default adalah pengetahuan publik. Dengan menentukan nama pengguna admin kustom, Anda dapat, misalnya, membantu mengurangi risiko atau efektivitas serangan brute force terhadap namespace.

Remediasi

Anda dapat mengubah nama pengguna admin untuk namespace Amazon Redshift Tanpa Server dengan menggunakan konsol Amazon Redshift Serverless atau API. Untuk mengubahnya menggunakan konsol, pilih konfigurasi namespace, lalu pilih Edit kredensyal admin di menu Tindakan. Untuk mengubahnya secara terprogram, gunakan UpdateNamespaceoperasi atau, jika Anda menggunakanAWS CLI, jalankan perintah update-namespace. Jika Anda mengubah nama pengguna admin, Anda juga harus mengubah kata sandi admin secara bersamaan.

[RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::RedshiftServerless::Namespace`

AWS Configaturan: redshift-serverless-publish-logs-to-cloudwatch

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah namespace Amazon Redshift Tanpa Server dikonfigurasi untuk mengekspor koneksi dan log pengguna ke Amazon Logs. CloudWatch Kontrol gagal jika namespace Redshift Tanpa Server tidak dikonfigurasi untuk mengekspor log ke Log. CloudWatch

Jika Anda mengonfigurasi Amazon Redshift Tanpa Server untuk mengekspor data log koneksi (`connectionlog`) dan log pengguna (`userlog`) ke grup log di Amazon CloudWatch Logs, Anda dapat mengumpulkan dan menyimpan catatan log Anda dalam penyimpanan tahan lama, yang dapat mendukung ulasan dan audit keamanan, akses, dan ketersediaan. Dengan CloudWatch Log, Anda juga dapat melakukan analisis real-time data log dan digunakan CloudWatch untuk membuat alarm dan meninjau metrik.

Remediasi

Untuk mengekspor data log untuk namespace Amazon Redshift Tanpa Server ke Amazon CloudWatch Logs, masing-masing log harus dipilih untuk diekspor dalam pengaturan konfigurasi pencatatan audit untuk namespace. Untuk informasi tentang memperbarui setelan ini, lihat Mengedit keamanan dan enkripsi di Panduan Manajemen Amazon Redshift.

Kontrol CSPM Security Hub untuk Route 53

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Route 53.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Route53::HealthCheck`

AWS Configaturan: `tagged-route53-healthcheck` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah pemeriksaan kesehatan Amazon Route 53 memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika pemeriksaan kesehatan tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika pemeriksaan kesehatan tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke pemeriksaan kesehatan Route 53, lihat Penamaan dan penandaan pemeriksaan kesehatan di Panduan Pengembang Amazon Route 53.

[Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Route53::HostedZone`

AWS Configaturan: **`route53-query-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan kueri DNS diaktifkan untuk zona host publik Amazon Route 53. Kontrol gagal jika pencatatan kueri DNS tidak diaktifkan untuk zona host publik Route 53.

Mencatat kueri DNS untuk zona yang dihosting Route 53 memenuhi persyaratan keamanan dan kepatuhan DNS dan memberikan visibilitas. Log mencakup informasi seperti domain atau subdomain yang ditanyakan, tanggal dan waktu kueri, jenis catatan DNS (misalnya, A atau AAAA), dan kode respons DNS (misalnya, atau). `NoError` `ServFail` Saat pencatatan kueri DNS diaktifkan, Route 53 menerbitkan file log ke Amazon CloudWatch Logs.

Remediasi

Untuk mencatat kueri DNS untuk zona host publik Route 53, lihat Mengonfigurasi pencatatan untuk kueri DNS di Panduan Pengembang Amazon Route 53.

Kontrol CSPM Hub Keamanan untuk Amazon S3

AWS Security Hub CSPM Kontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Storage Service (Amazon S3). Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.1.4, Benchmark Yay AWS asan CIS v3.0. 0/2.1.4, Benchmark Yay AWS asan CIS v1.4. 0/2.1.5, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: s3-account-level-public-access-blocks-periodic

Jenis jadwal: Ber kala

Parameter:

- `ignorePublicAcls`: `true` (tidak dapat disesuaikan)
- `blockPublicPolicy`: `true` (tidak dapat disesuaikan)
- `blockPublicAcls`: `true` (tidak dapat disesuaikan)
- `restrictPublicBuckets`: `true` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah setelan akses publik blok Amazon S3 sebelumnya dikonfigurasi pada tingkat akun untuk bucket tujuan umum S3. Kontrol gagal jika satu atau lebih pengaturan akses publik blok diatur ke`false`.

Kontrol gagal jika salah satu pengaturan diatur ke`false`, atau jika salah satu pengaturan tidak dikonfigurasi.

Blok akses publik Amazon S3 dirancang untuk menyediakan kontrol di seluruh Akun AWS atau pada tingkat bucket S3 individual untuk memastikan bahwa objek tidak pernah memiliki akses publik. Akses publik diberikan kepada bucket dan objek melalui daftar kontrol akses (ACL), kebijakan bucket, atau keduanya.

Kecuali Anda ingin bucket S3 Anda dapat diakses publik, Anda harus mengonfigurasi fitur Amazon S3 Block Public Access tingkat akun.

Untuk mempelajari selengkapnya, lihat Menggunakan Amazon S3 Memblokir Akses Pu blik di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Remediasi

Untuk mengaktifkan Akses Publik Blok Amazon S3 untuk Anda Akun AWS, lihat Meng onfigurasi setelan akses publik blok untuk akun Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-public-read-prohibited

Jenis jadwal: Periodik dan perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengizinkan akses baca publik. Ini mengevaluasi pengaturan akses publik blok, kebijakan bucket, dan daftar kontrol akses bucket (ACL). Kontrol gagal jika bucket mengizinkan akses baca publik.

> **Note**
>
> Jika bucket S3 memiliki kebijakan bucket, kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan tem `PASSED` uan, kondisi dalam kebijakan bucket hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat Variabel dan tag di Panduan AWS Identity and Access Management Pengguna.

Beberapa kasus penggunaan mungkin mengharuskan semua orang di internet dapat membaca dari bucket S3 Anda. Namun, situasi tersebut jarang terjadi. Untuk memastikan integritas dan keamanan data Anda, bucket S3 Anda tidak boleh dibaca publik.

Remediasi

Untuk memblokir akses baca publik di bucket Amazon S3 Anda, lihat Mengon figurasi setelan akses publik blok untuk bucket S3 Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik

Persyaratan terkait: PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v3.2. 1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-public-write-prohibited

Jenis jadwal: Periodik dan perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengizinkan akses penulisan publik. Ini mengevaluasi pengaturan akses publik blok, kebijakan bucket, dan daftar kontrol akses bucket (ACL). Kontrol gagal jika bucket mengizinkan akses tulis publik.

> **Note**
>
> Jika bucket S3 memiliki kebijakan bucket, kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan tem `PASSED` uan, kondisi dalam kebijakan bucket hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak mengandung karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat Variabel dan tag di Panduan AWS Identity and Access Management Pengguna.

Beberapa kasus penggunaan mengharuskan semua orang di internet dapat menulis ke bucket S3 Anda. Namun, situasi tersebut jarang terjadi. Untuk memastikan integritas dan keamanan data Anda, bucket S3 Anda tidak boleh ditulis secara publik.

Remediasi

Untuk memblokir akses tulis publik di bucket Amazon S3 Anda, lihat Mengon figurasi setelan akses publik blok untuk bucket S3 Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.1.1, Benchmark Yay AWS asan CIS v3.0. 0/2.1.1, Benchmark Yay AWS asan CIS v1.4. 0/2.1.2, NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3),, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3) NIST.800-53.r5 SC-23, (4),, NIST.800-53.r5 SC-7 (1) NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v3.2. 1/4.1, PCI DSS v4.0. 1/4.2.1

Kategori: Lindungi > Manajemen akses aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-ssl-requests-only

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memiliki kebijakan yang mengharuskan permintaan untuk menggunakan TLS. Kontrol gagal jika kebijakan bucket tidak memerlukan permintaan untuk menggunakan TLS.

Bucket S3 harus memiliki kebijakan yang mengharuskan semua permintaan (`Action: S3:*`) untuk hanya menerima transmisi data melalui HTTPS dalam kebijakan sumber daya S3, yang ditunjukkan oleh kunci kondisi`aws:SecureTransport`.

Remediasi

Untuk memperbarui kebijakan bucket Amazon S3 untuk menolak transportasi tidak aman, lihat Men ambahkan kebijakan bucket dengan menggunakan konsol Amazon S3 di Panduan Pengguna Layanan Peny impanan Sederhana Amazon.

Tambahkan pernyataan kebijakan yang mirip dengan yang ada di kebijakan berikut. Ganti `amzn-s3-demo-bucket` dengan nama bucket yang Anda modifikasi.

JSON

```
{
    "Id": "ExamplePolicy",
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSSLRequestsOnly",
            "Action": "s3:*",
            "Effect": "Deny",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ],
            "Condition": {
                "Bool": {
                     "aws:SecureTransport": "false"
                }
            },
           "Principal": "*"
```

```
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Kebijakan bucket S3 apa yang harus saya gunakan untuk mematuhi AWS Config aturan s3-bucket-ssl-requests-only? di Pusat Peng AWS etahuan Resmi.

[S3.6] Kebijakan bucket tujuan umum S3 harus membatasi akses ke yang lain Akun AWS

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.4

Kategori: L indungi > Manajemen akses aman > Tindakan operasi API sensitif dibatasi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::S3::Bucket`

AWS Configaturan: s3-bucket-blacklisted-actions-prohibited

Jenis jadwal: Perubahan dipicu

Parameter:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah kebijakan bucket tujuan umum Amazon S3 mencegah prinsipal dari pihak lain Akun AWS melakukan tindakan yang ditolak pada sumber daya di bucket S3. Kontrol gagal jika kebijakan bucket mengizinkan satu atau lebih tindakan sebelumnya untuk prinsipal di yang lain Akun AWS.

Menerapkan akses hak istimewa paling sedikit sangat penting untuk mengurangi risiko keamanan dan dampak kesalahan atau niat jahat. Jika kebijakan bucket S3 mengizinkan akses dari akun eksternal, hal itu dapat mengakibatkan eksfiltrasi data oleh ancaman orang dalam atau penyerang.

`blacklistedactionpatterns`Parameter memungkinkan evaluasi aturan untuk bucket S3 yang berhasil. Parameter memberikan akses ke akun eksternal untuk pola tindakan yang tidak termasuk dalam `blacklistedactionpatterns` daftar.

Remediasi

Untuk memperbarui kebijakan bucket Amazon S3 untuk menghapus izin, lihat. Menambahkan kebijakan bucket dengan menggunakan konsol Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Di halaman Edit kebijakan bucket, di kotak teks pengeditan kebijakan, lakukan salah satu tindakan berikut:

- Hapus pernyataan yang memberikan Akun AWS akses lain ke tindakan yang ditolak.
- Hapus tindakan yang ditolak yang diizinkan dari pernyataan.

[S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah

Persyaratan terkait: PCI DSS v3.2. 1/2.2, NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-36 (2), NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Lindungi > Manajemen akses aman

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-cross-region-replication-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan replikasi lintas wilayah. Kontrol gagal jika bucket tidak mengaktifkan replikasi lintas wilayah.

Replikasi adalah penyalinan objek secara otomatis dan asinkron di seluruh bucket yang sama atau berbeda. Wilayah AWS Replikasi menyalin objek yang baru dibuat dan pembaruan objek dari bucket sumber ke bucket tujuan atau bucket. AWS praktik terbaik merekomendasikan replikasi untuk bucket sumber dan tujuan yang dimiliki oleh yang sama Akun AWS. Selain ketersediaan, Anda harus mempertimbangkan pengaturan pengerasan sistem lainnya.

Kontrol ini menghasilkan tem `FAILED` uan untuk bucket tujuan replikasi jika replikasi lintas wilayah tidak diaktifkan. Jika ada alasan yang sah bahwa bucket tujuan tidak memerlukan replikasi lintas wilayah untuk diaktifkan, Anda dapat menekan temuan untuk bucket ini.

Remediasi

Untuk mengaktifkan Cross-Region Replikasi pada bucket S3, lihat Meng onfigurasi replikasi untuk bucket sumber dan tujuan yang dimiliki oleh akun yang sama di Panduan Pengguna Amazon Simple Storage Service. Untuk Bucket Sumber, pilih Terapkan ke semua objek dalam bucket.

[S3.8] Bucket tujuan umum S3 harus memblokir akses publik

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.1.4, Benchmark Yayasan CIS AWS v3.0.02.1.4, Tolok Ukur Yayasan CIS v1.4. AWS 0/2.1.5, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: Melindungi > Manajemen akses aman > Kontrol akses

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-level-public-access-prohibited

Jenis jadwal: Perubahan dipicu

Parameter:

- `excludedPublicBuckets`(tidak dapat disesuaikan) - Daftar nama bucket S3 publik yang diketahui diizinkan dengan koma

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memblokir akses publik di tingkat bucket. Kontrol gagal jika salah satu pengaturan berikut diatur ke`false`:

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Blokir Akses Publik di tingkat bucket S3 menyediakan kontrol untuk memastikan bahwa objek tidak pernah memiliki akses publik. Akses publik diberikan kepada bucket dan objek melalui daftar kontrol akses (ACL), kebijakan bucket, atau keduanya.

Kecuali Anda ingin bucket S3 Anda dapat diakses secara publik, Anda harus mengonfigurasi fitur Amazon S3 Block Public Access tingkat bucket.

Remediasi

Untuk informasi tentang cara menghapus akses publik di tingkat bucket, lihat Mem blokir akses publik ke penyimpanan Amazon S3 Anda di Panduan Pengguna Amazon S3.

[S3.9] Bucket tujuan umum S3 harus mengaktifkan logging akses server

Persyaratan terkait: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.3.8, PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging akses server diaktifkan untuk bucket tujuan umum Amazon S3. Kontrol gagal jika logging akses server tidak diaktifkan. Saat logging diaktifkan, Amazon S3 mengirimkan log akses untuk bucket sumber ke bucket target yang dipilih. Bucket target harus Wilayah AWS sama dengan bucket sumber dan tidak boleh memiliki periode retensi default yang dikonfigurasi. Bucket logging target tidak perlu mengaktifkan logging akses server, dan Anda harus menekan temuan untuk bucket ini.

Pencatatan akses server menyediakan catatan terperinci dari permintaan yang dibuat ke bucket. Log akses server dapat membantu dalam audit keamanan dan akses. Untuk informasi selengkapnya, lihat Praktik Terbaik Keamanan untuk Amazon S3: Mengaktifkan pencatatan akses server Amazon S3.

Remediasi

Untuk mengaktifkan logging akses server Amazon S3, lihat Mengaktifkan log akses server Amazon S3 di Panduan Pengguna Amazon S3.

[S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-version-lifecycle-policy-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket berversi tujuan umum Amazon S3 memiliki konfigurasi Siklus Hidup. Kontrol gagal jika bucket tidak memiliki konfigurasi Siklus Hidup.

Sebaiknya buat konfigurasi Siklus Hidup untuk bucket S3 untuk membantu menentukan tindakan yang ingin dilakukan Amazon S3 selama masa pakai objek.

> **Tip**
>
> Mengaktifkan pembuatan versi tanpa manajemen siklus hidup dapat menyebabkan pertumbuhan penyimpanan tanpa batas dan peningkatan biaya. Setiap modifikasi objek menciptakan versi baru yang dipertahankan tanpa batas waktu. Konfigurasikan aturan Siklus Hidup S3 untuk secara otomatis mengalihkan versi noncurrent ke kelas penyimpanan yang lebih murah atau kedaluwarsa setelah periode retensi yang ditentukan.

Remediasi

Untuk informasi selengkapnya tentang mengonfigurasi siklus hidup pada bucket Amazon S3, lihat Menggunakan Versi S3 dengan Siklus Siklus S3 , Mengatur konfigurasi siklus hidup pada bucket, dan M engelola siklus hidup objek di Panduan Pengguna Amazon S3.

[S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa

Persyaratan terkait: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (4), NIST.800-171.r2 3.3.8

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-event-notifications-enabled

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`eventTypes`	Daftar jenis acara S3 yang disukai	EnumList (maksimal 28 item)	`s3:IntelligentTiering`, `s3:LifecycleExpiration:*`, `s3:LifecycleExpiration:Delete`, `s3:LifecycleExpiration:DeleteMarkerCreated`, `s3:LifecycleTransition`,	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
			s3:ObjectAcl:Put, s3:ObjectCreated:*, s3:ObjectCreated:CompleteMultipartUpload, s3:ObjectCreated:Copy, s3:ObjectCreated:Post, s3:ObjectCreated:Put, s3:ObjectRemoved:*, s3:ObjectRemoved:Delete, s3:ObjectRemoved:DeleteMarkerCreated, s3:ObjectRestore:*	

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
			, s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:* , s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:Ope	

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
			`rationMissedThreshold`, `s3:Replication:OperationNotTracked`, `s3:Replication:OperationReplicatedAfterThreshold`, `s3:TestEvent`	

Kontrol ini memeriksa apakah Notifikasi Peristiwa S3 diaktifkan pada bucket tujuan umum Amazon S3. Kontrol gagal jika Notifikasi Peristiwa S3 tidak diaktifkan di bucket. Jika Anda memberikan nilai kustom untuk `eventTypes` parameter, kontrol hanya akan diteruskan jika notifikasi peristiwa diaktifkan untuk jenis peristiwa yang ditentukan.

Saat mengaktifkan Notifikasi Peristiwa S3, Anda menerima peringatan ketika peristiwa tertentu terjadi yang memengaruhi bucket S3 Anda. Misalnya, Anda dapat diberitahu tentang pembuatan objek, penghapusan objek, dan pemulihan objek. Pemberitahuan ini dapat mengingatkan tim terkait tentang modifikasi yang tidak disengaja atau disengaja yang dapat menyebabkan akses data yang tidak sah.

Remediasi

Untuk informasi tentang mendeteksi perubahan pada bucket dan objek S3, lihat Pem beritahuan Peristiwa Amazon S3 di Panduan Pengguna Amazon S3.

[S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3

Persyaratan terkait: NIST.800-53.r5 AC-2 (1) NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Kategori: Melindungi > Manajemen akses aman > Kontrol akses

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-acl-prohibited

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 menyediakan izin pengguna dengan daftar kontrol akses (ACL). Kontrol gagal jika ACL dikonfigurasi untuk mengelola akses pengguna pada bucket.

ACL adalah mekanisme kontrol akses warisan yang mendahului IAM. Alih-alih ACL, sebaiknya gunakan kebijakan bucket S3 atau kebijakan AWS Identity and Access Management (IAM) untuk mengelola akses ke bucket S3 Anda.

Remediasi

Untuk melewati kontrol ini, Anda harus menonaktifkan ACL untuk bucket S3 Anda. Untuk petunjuk, lihat Meng ontrol kepemilikan objek dan menonaktifkan ACL untuk bucket Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk membuat kebijakan bucket S3, lihat Men ambahkan kebijakan bucket menggunakan konsol Amazon S3. Untuk membuat kebijakan pengguna IAM pada bucket S3, lihat Mengon trol akses ke bucket dengan kebijakan pengguna.

[S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Kategori: L indungi > Perlindungan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-lifecycle-policy-check

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`targetTransitionDays`	Jumlah hari setelah pembuatan objek ketika objek dialihkan ke kelas penyimpanan tertentu	Bilangan Bulat	`1` untuk `36500`	Tidak ada nilai default
`targetExpirationDays`	Jumlah hari setelah pembuatan objek saat objek dihapus	Bilangan Bulat	`1` untuk `36500`	Tidak ada nilai default
`targetTransitionStorageClass`	Tipe kelas penyimpanan S3 tujuan	Enum	`STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE`	Tidak ada nilai default

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 memiliki konfigurasi Siklus Hidup. Kontrol gagal jika bucket tidak memiliki konfigurasi Siklus Hidup. Jika Anda memberikan nilai kustom untuk satu atau beberapa parameter sebelumnya, kontrol akan diteruskan hanya jika kebijakan menyertakan kelas penyimpanan, waktu penghapusan, atau waktu transisi yang ditentukan.

Membuat konfigurasi Siklus Hidup untuk bucket S3 menentukan tindakan yang Anda ingin Amazon S3 lakukan selama masa pakai objek. Misalnya, Anda dapat mentransisikan objek ke kelas penyimpanan lain, mengarsipkannya, atau menghapusnya setelah jangka waktu tertentu.

Remediasi

Untuk informasi tentang mengonfigurasi kebijakan siklus hidup pada bucket Amazon S3, lihat Mengatur konfigurasi siklus hidup pada bucket dan lihat Mengelola siklus hidup penyimpanan Anda di Panduan Pengguna Amazon S3.

[S3.14] Bucket tujuan umum S3 harus mengaktifkan pembuatan versi

Kategori: Mel indungi > Perlindungan data > Perlindungan penghapusan data

Persyaratan terkait: NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), (2) NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5), NIST.800-171.r2 3.3.8

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-versioning-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan pembuatan versi. Kontrol gagal jika pembuatan versi ditangguhkan untuk bucket.

Pembuatan versi menyimpan beberapa varian objek di bucket S3 yang sama. Anda dapat menggunakan pembuatan versi untuk mempertahankan, mengambil, dan memulihkan semua versi dari semua objek yang disimpan di bucket S3 Anda. Pembuatan versi membantu Anda memulihkan dari tindakan pengguna yang tidak diinginkan dan kegagalan aplikasi.

> **Tip**
>
> Mengaktifkan pembuatan versi tanpa manajemen siklus hidup dapat menyebabkan pertumbuhan penyimpanan tanpa batas dan peningkatan biaya. Setiap modifikasi objek menciptakan versi baru yang dipertahankan tanpa batas. Konfigurasikan aturan Siklus Hidup S3 untuk secara otomatis mengalihkan versi noncurrent ke kelas penyimpanan yang

lebih murah atau kedaluwarsa setelah periode retensi yang ditentukan. Untuk informasi selengkapnya, lihat Menggunakan Versi S3 dengan Siklus Siklus S3 dan M engelola siklus hidup objek.

Remediasi

Untuk menggunakan pembuatan versi pada bucket S3, lihat Meng aktifkan pembuatan versi pada bucket di Panduan Pengguna Amazon S3.

[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock

Kategori: Mel indungi > Perlindungan data > Perlindungan penghapusan data

Persyaratan terkait: NIST.800-53.r5 CP-6 (2), PCI DSS v4.0. 1/10.5.1

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-default-lock-enabled

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`mode`	Mode retensi Kunci Objek S3	Enum	`GOVERNANCE`, `COMPLIANCE`	Tidak ada nilai default

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 mengaktifkan Object Lock. Kontrol gagal jika Object Lock tidak diaktifkan untuk bucket. Jika Anda memberikan nilai kustom untuk `mode` parameter, kontrol hanya akan lolos jika S3 Object Lock menggunakan mode retensi yang ditentukan.

Anda dapat menggunakan S3 Object Lock untuk menyimpan objek menggunakan model write-once-read-many (WORM). Object Lock dapat membantu mencegah objek dalam bucket S3 dihapus

atau diganti untuk jangka waktu tertentu atau tanpa batas waktu. Anda dapat menggunakan S3 Object Lock untuk memenuhi persyaratan peraturan yang memerlukan penyimpanan WORM, atau menambahkan lapisan perlindungan tambahan terhadap perubahan dan penghapusan objek.

Remediasi

Untuk mengonfigurasi Object Lock untuk bucket S3 baru dan yang sudah ada, lihat Mengonfigurasi Kunci Objek S3 di Panduan Pengguna Amazon S3.

[S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Persyaratan terkait: NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), (10), NIST.800-53.r5 SC-7 (1), NIST.800-53.r5 CA-9 NIST.800-53.r5 SI-7 (6),, NIST.800-171.r2 3.8.9 NIST.800-53.r5 AU-9, 3. NIST.800-171.r2 13.11, NIST.800-171.r2 3.13.16, PCI DSS v4.0. 1/3.5.1

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-default-encryption-kms

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah bucket tujuan umum Amazon S3 dienkripsi dengan AWS KMS key (SSE-KMS atau DSSE-KMS). Kontrol gagal jika bucket dienkripsi dengan enkripsi default (SSE-S3).

Server-side Enkripsi (SSE) adalah enkripsi data di tujuannya oleh aplikasi atau layanan yang menerimanya. Kecuali Anda menentukan sebaliknya, bucket S3 menggunakan kunci terkelola Amazon S3 (SSE-S3) secara default untuk enkripsi sisi server. Namun, untuk kontrol tambahan, Anda dapat memilih untuk mengonfigurasi bucket untuk menggunakan enkripsi sisi server dengan AWS KMS keys (SSE-KMS atau DSSE-KMS) sebagai gantinya. Amazon S3 mengenkripsi data Anda di tingkat objek saat menulisnya ke disk di pusat AWS data dan mendekripsi untuk Anda saat Anda mengaksesnya.

Remediasi

Untuk mengenkripsi bucket S3 menggunakan SSE-KMS, lihat Men entukan enkripsi sisi server dengan AWS KMS (SSE-KMS) di Panduan Pengguna Amazon S3. Untuk mengenkripsi bucket S3

menggunakan DSSE-KMS, lihat Men entukan enkripsi sisi server lapis ganda dengan AWS KMS keys (DSSE-KMS) di Panduan Pengguna Amazon S3.

[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::S3::AccessPoint`

AWS Config aturan: s3-access-point-public-access-blocks

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah titik akses Amazon S3 telah mengaktifkan setelan akses publik blokir. Kontrol gagal jika pengaturan akses publik blokir tidak diaktifkan untuk titik akses.

Fitur Amazon S3 Block Public Access membantu Anda mengelola akses ke sumber daya S3 Anda di tiga tingkat: level akun, bucket, dan titik akses. Pengaturan di setiap level dapat dikonfigurasi secara independen, memungkinkan Anda memiliki tingkat pembatasan akses publik yang berbeda untuk data Anda. Pengaturan titik akses tidak dapat secara individual mengganti pengaturan yang lebih ketat di level yang lebih tinggi (tingkat akun atau bucket yang ditetapkan ke titik akses). Sebaliknya, pengaturan pada tingkat titik akses bersifat aditif, artinya mereka melengkapi dan bekerja bersama pengaturan di level lain. Kecuali jika Anda ingin titik akses S3 dapat diakses publik, Anda harus mengaktifkan pengaturan akses publik blokir.

Remediasi

Saat ini, Amazon S3 tidak mendukung perubahan pengaturan akses publik blokir titik akses setelah titik akses dibuat. Semua pengaturan akses publik blok diaktifkan secara default saat Anda membuat titik akses baru. Kami menyarankan Anda tetap mengaktifkan semua pengaturan kecuali Anda tahu bahwa Anda memiliki kebutuhan khusus untuk menonaktifkan salah satu pengaturan tersebut. Untuk

informasi selengkapnya, lihat Mengelola akses publik ke titik akses di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/2.1.2, Benchmark Yay AWS asan CIS v3.0. 0/2.1.2, Benchmark Yay AWS asan CIS v1.4. 0/2.1.3, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Kategori: Mel indungi > Perlindungan data > Perlindungan penghapusan data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3::Bucket`

AWS Config aturan: s3-bucket-mfa-delete-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah penghapusan autentikasi multi-faktor (MFA) diaktifkan untuk bucket tujuan umum Amazon S3. Kontrol gagal jika penghapusan MFA tidak diaktifkan untuk bucket. Kontrol tidak menghasilkan temuan untuk bucket yang memiliki konfigurasi siklus hidup.

Jika Anda mengaktifkan pembuatan versi untuk bucket tujuan umum S3, Anda dapat menambahkan lapisan keamanan lain secara opsional dengan mengonfigurasi penghapusan MFA untuk bucket. Jika Anda melakukan ini, pemilik bucket harus menyertakan dua bentuk otentikasi dalam permintaan apa pun untuk menghapus versi objek dalam bucket atau mengubah status versi bucket. Penghapusan MFA memberikan keamanan tambahan jika, misalnya, kredentif keamanan pemilik bucket dikompromikan. Penghapusan MFA juga dapat membantu mencegah penghapusan bucket yang tidak disengaja dengan mengharuskan pengguna yang memulai tindakan hapus untuk membuktikan kepemilikan fisik perangkat MFA dengan kode MFA, yang menambahkan lapisan gesekan dan keamanan ekstra pada tindakan penghapusan.

> **Note**
>
> Kontrol ini menghasilkan tem `PASSED` uan hanya jika penghapusan MFA diaktifkan untuk bucket tujuan umum S3. Untuk mengaktifkan penghapusan MFA untuk bucket, pembuatan versi juga harus diaktifkan untuk bucket. Bucket versioning adalah metode untuk menyimpan beberapa variasi objek S3 dalam bucket yang sama. Selain itu, hanya pemilik bucket yang

masuk sebagai pengguna root yang dapat mengaktifkan penghapusan MFA dan melakukan tindakan hapus pada bucket. Anda tidak dapat menggunakan penghapusan MFA dengan bucket yang memiliki konfigurasi siklus hidup.

Remediasi

Untuk informasi tentang mengaktifkan pembuatan versi dan mengonfigurasi penghapusan MFA untuk bucket S3, lihat Meng konfigurasi penghapusan MFA di Panduan Pengguna Amazon Simple Storage Service.

[S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/3.8, Benchmark Yay AWS asan CIS v3.0. 0/3.8, PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: cloudtrail-all-write-s3-data-event-check

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah an Akun AWS memiliki setidaknya satu jejak AWS CloudTrail Multi-wilayah yang mencatat semua peristiwa data penulisan untuk bucket Amazon S3. Kontrol gagal jika akun tidak memiliki jejak Multi-wilayah yang mencatat peristiwa data penulisan untuk bucket S3.

Operasi tingkat objek S3, sepertiGetObject,DeleteObject, danPutObject, disebut peristiwa data. Secara default, CloudTrail tidak mencatat peristiwa data, tetapi Anda dapat mengonfigurasi jejak untuk mencatat peristiwa data untuk bucket S3. Saat Anda mengaktifkan logging tingkat objek untuk peristiwa data tulis, Anda dapat mencatat setiap akses objek (file) individu dalam bucket S3. Mengaktifkan logging tingkat objek dapat membantu Anda memenuhi persyaratan kepatuhan data, melakukan analisis keamanan komprehensif, memantau pola perilaku pengguna tertentu di Anda Akun AWS, dan mengambil tindakan pada aktivitas API tingkat objek dalam bucket S3 Anda dengan menggunakan Amazon Events. CloudWatch Kontrol ini menghasilkan tem PASSED uan jika Anda mengonfigurasi jejak Multi-wilayah yang mencatat hanya tulis atau semua jenis peristiwa data untuk semua bucket S3.

Remediasi

Untuk mengaktifkan logging tingkat objek untuk bucket S3, lihat Meng aktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3 di Panduan Pengguna Amazon Simple Storage Service.

[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek

Persyaratan terkait: CIS Foun AWS dations Benchmark v5.0. 0/3.9, Benchmark Yay AWS asan CIS v3.0. 0/3.9, PCI DSS v4.0. 1/10.2.1

Kategori: Identifikasi > Pencatatan

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Config aturan: cloudtrail-all-read-s3-data-event-check

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah an Akun AWS memiliki setidaknya satu jejak AWS CloudTrail Multi-wilayah yang mencatat semua peristiwa data baca untuk bucket Amazon S3. Kontrol gagal jika akun tidak memiliki jejak Multi-wilayah yang mencatat peristiwa data baca untuk bucket S3.

Operasi tingkat objek S3, sepertiGetObject,DeleteObject, danPutObject, disebut peristiwa data. Secara default, CloudTrail tidak mencatat peristiwa data, tetapi Anda dapat mengonfigurasi jejak untuk mencatat peristiwa data untuk bucket S3. Saat Anda mengaktifkan logging tingkat objek untuk peristiwa data baca, Anda dapat mencatat setiap akses objek (file) individu dalam bucket S3. Mengaktifkan logging tingkat objek dapat membantu Anda memenuhi persyaratan kepatuhan data, melakukan analisis keamanan komprehensif, memantau pola perilaku pengguna tertentu di Anda Akun AWS, dan mengambil tindakan pada aktivitas API tingkat objek dalam bucket S3 Anda dengan menggunakan Amazon Events. CloudWatch Kontrol ini menghasilkan tem PASSED uan jika Anda mengonfigurasi jejak Multi-wilayah yang mencatat read-only atau semua jenis peristiwa data untuk semua bucket S3.

Remediasi

Untuk mengaktifkan logging tingkat objek untuk bucket S3, lihat Meng aktifkan pencatatan CloudTrail peristiwa untuk bucket dan objek S3 di Panduan Pengguna Amazon Simple Storage Service.

[S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok

Persyaratan terkait: PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::S3::MultiRegionAccessPoint`

AWS Config aturan: `s3-mrap-public-access-blocked` (aturan CSPM Hub Keamanan kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah Titik Akses Amazon S3 Multi-Region telah mengaktifkan setelan akses publik blokir. Kontrol gagal saat T Multi-Region itik Akses tidak mengaktifkan pengaturan akses publik blokir.

Sumber daya yang dapat diakses publik dapat menyebabkan akses tidak sah, pelanggaran data, atau eksploitasi kerentanan. Membatasi akses melalui langkah-langkah otentikasi dan otorisasi membantu melindungi informasi sensitif dan menjaga integritas sumber daya Anda.

Remediasi

Secara default, semua setelan Blok Akses Publik diaktifkan untuk Titik Multi-Region Akses S3. Untuk informasi selengkapnya, lihat Memblokir akses publik dengan Titik Ak Multi-Region ses Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. Anda tidak dapat mengubah setelan Blokir Akses Pu Multi-Region blik untuk Titik Akses setelah dibuat.

[S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup

Kategori: Mel indungi > Perlindungan Data

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::S3Express::DirectoryBucket`

AWS Config aturan: s3express-dir-bucket-lifecycle-rules-check

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`targetExpirationDays`	Jumlah hari, setelah pembuatan objek, ketika objek harus kedaluwarsa.	Bilangan Bulat	1 untuk 2147483647	Tidak ada nilai default

Kontrol ini memeriksa apakah aturan siklus hidup dikonfigurasi untuk bucket direktori S3. Kontrol gagal jika aturan siklus hidup tidak dikonfigurasi untuk bucket direktori, atau aturan siklus hidup untuk bucket menentukan setelan kedaluwarsa yang tidak cocok dengan nilai parameter yang Anda tentukan secara opsional.

Di Amazon S3, konfigurasi siklus hidup adalah seperangkat aturan yang menentukan tindakan untuk Amazon S3 untuk diterapkan ke sekelompok objek dalam bucket. Untuk bucket direktori S3, Anda dapat membuat aturan siklus hidup yang menentukan kapan objek kedaluwarsa berdasarkan usia (dalam hari). Anda juga dapat membuat aturan siklus hidup yang menghapus unggahan multipart yang tidak lengkap. Tidak seperti jenis bucket S3 lainnya, seperti bucket tujuan umum, bucket direktori tidak mendukung jenis tindakan lain untuk aturan siklus hidup, seperti transisi objek antar kelas penyimpanan.

Remediasi

Untuk menentukan konfigurasi siklus hidup untuk bucket direktori S3, buat aturan siklus hidup untuk bucket. Untuk informasi selengkapnya, lihat Membuat dan mengelola konfigurasi siklus hidup untuk bucket direktori Anda di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Kontrol CSPM Hub Keamanan untuk AI SageMaker

AWS Security Hub CSPM Kontrol ini mengevaluasi layanan dan sumber daya Amazon SageMaker AI. Kontrol mungkin tidak tersedia di semua Wilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,

NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9), PCI DSS v3.2. 1/1.2.1, PCI DSS v3.2. 1/1.3.1, PCI DSS v3.2. 1/1.3.2, PCI DSS v3.2. 1/1.3.4, PCI DSS v3.2. 1/1.3.6, PCI DSS v4.0. 1/1.4.4

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: sagemaker-notebook-no-direct-internet-access

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses internet langsung dinonaktifkan untuk instance notebook SageMaker AI. Kontrol gagal jika `DirectInternetAccess` bidang diaktifkan untuk instance notebook.

Jika Anda mengonfigurasi instans SageMaker AI tanpa VPC, maka secara default akses internet langsung diaktifkan pada instans Anda. Anda harus mengonfigurasi instance Anda dengan VPC dan mengubah pengaturan default menjadi Nonaktifkan —Akses internet melalui VPC. Untuk melatih atau meng-host model dari notebook, Anda memerlukan akses internet. Untuk mengaktifkan akses internet, VPC Anda harus memiliki titik akhir antarmuka (AWS PrivateLink) atau gateway NAT dan grup keamanan yang memungkinkan koneksi keluar. Untuk mempelajari selengkapnya tentang cara menghubungkan instance notebook ke sumber daya di VPC, lihat Menyam bungkan instance notebook ke sumber daya di VPC di Panduan Pengembang SageMaker AI Amazon. Anda juga harus memastikan bahwa akses ke konfigurasi SageMaker AI Anda terbatas hanya untuk pengguna yang berwenang. Batasi izin IAM yang memungkinkan pengguna mengubah pengaturan dan sumber daya SageMaker AI.

Remediasi

Anda tidak dapat mengubah pengaturan akses internet setelah membuat instance buku catatan. Sebagai gantinya, Anda dapat menghentikan, menghapus, dan membuat ulang instance dengan akses internet yang diblokir. Untuk menghapus instans buku catatan yang mengizinkan akses internet langsung, lihat Menggunakan instance notebook untuk membuat model: Membersihkan di Panduan Pengembang SageMaker AI Amazon. Untuk membuat ulang instance buku catatan

yang menolak akses internet, lihat Membuat instance buku catatan. Untuk Jaringan, Akses internet langsung, pilih Non aktifkan—Akses internet melalui VPC.

[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya dalam VPC

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: sagemaker-notebook-instance-inside-vpc

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance notebook Amazon SageMaker AI diluncurkan dalam cloud pribadi virtual khusus (VPC). Kontrol ini gagal jika instance notebook SageMaker AI tidak diluncurkan dalam VPC khusus atau jika diluncurkan di layanan SageMaker AI VPC.

Subnet adalah rentang alamat IP dalam VPC. Sebaiknya simpan sumber daya Anda di dalam VPC kustom bila memungkinkan untuk memastikan perlindungan jaringan yang aman dari infrastruktur Anda. Amazon VPC adalah jaringan virtual yang didedikasikan untuk Anda Akun AWS. Dengan Amazon VPC, Anda dapat mengontrol akses jaringan dan konektivitas internet SageMaker AI Studio dan instance notebook Anda.

Remediasi

Anda tidak dapat mengubah setelan VPC setelah membuat instance buku catatan. Sebagai gantinya, Anda dapat menghentikan, menghapus, dan membuat ulang instance. Untuk petunjuk, lihat Menggunakan instance notebook untuk membuat model: Membersihkan di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Kategori: Lindungi > Manajemen akses aman > Pembatasan akses pengguna root

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: sagemaker-notebook-instance-root-access-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah akses root diaktifkan untuk instance notebook Amazon SageMaker AI. Kontrol gagal jika akses root diaktifkan untuk instance notebook SageMaker AI.

Sesuai dengan prinsip hak istimewa terendah, praktik terbaik keamanan yang disarankan adalah membatasi akses root ke sumber daya instans untuk menghindari izin penyediaan berlebihan secara tidak sengaja.

Remediasi

Untuk membatasi akses root ke instans notebook SageMaker AI, lihat Mengontrol akses root ke instance notebook SageMaker AI di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1

Persyaratan terkait: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SA-13

Kategori: Pu lihkan > Ketahanan > Ketersediaan tinggi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::EndpointConfig`

AWS Config aturan: sagemaker-endpoint-config-prod-instance-count

Jenis jadwal: Ber kala

Parameter: Tidak ada

Kontrol ini memeriksa apakah varian produksi dari titik akhir Amazon SageMaker AI memiliki jumlah instans awal lebih besar dari 1. Kontrol gagal jika varian produksi titik akhir hanya memiliki 1 instance awal.

Varian produksi yang berjalan dengan jumlah instans lebih besar dari 1 memungkinkan redundansi instans multi-AZ yang dikelola oleh SageMaker AI. Menyebarkan sumber daya di beberapa Zona Ketersediaan adalah praktik AWS terbaik untuk memberikan ketersediaan tinggi dalam arsitektur Anda. Ketersediaan tinggi membantu Anda pulih dari insiden keamanan.

> **Note**
>
> Kontrol ini hanya berlaku untuk konfigurasi titik akhir berbasis instance.

Remediasi

Untuk informasi selengkapnya tentang parameter konfigurasi titik akhir, lihat Membuat konfigurasi titik akhir di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::Model`

AWS Config aturan: sagemaker-model-isolation-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah model yang dihosting Amazon SageMaker AI mengaktifkan isolasi jaringan. Kontrol gagal jika `EnableNetworkIsolation` parameter untuk model yang dihosting diatur ke`False`.

SageMaker Pelatihan AI dan wadah inferensi yang digunakan diaktifkan internet secara default. Jika Anda tidak ingin SageMaker AI menyediakan akses jaringan eksternal ke wadah pelatihan atau inferensi Anda, Anda dapat mengaktifkan isolasi jaringan. Jika Anda mengaktifkan isolasi jaringan, tidak ada panggilan jaringan masuk atau keluar yang dapat dilakukan ke atau dari wadah model, termasuk panggilan ke atau dari yang lain. Layanan AWS Selain itu, tidak ada AWS kredenSIAL yang tersedia untuk lingkungan runtime kontainer. Mengaktifkan isolasi jaringan membantu mencegah akses yang tidak diinginkan ke sumber daya SageMaker AI Anda dari internet.

> **Note**
>
> Pada 13 Agustus 2025, Security Hub CSPM mengubah judul dan deskripsi kontrol ini. Judul dan deskripsi baru lebih akurat mencerminkan bahwa kontrol memeriksa pengaturan untuk `EnableNetworkIsolation` parameter model yang di SageMaker hosting Amazon AI. Sebelumnya, judul kontrol ini adalah: SageMaker models should block inbound traffic.

Remediasi

Untuk informasi selengkapnya tentang isolasi jaringan untuk model SageMaker AI, lihat Menjalankan wadah pelatihan dan inferensi dalam mode bebas internet di Panduan Pengembang SageMaker AI Amazon. Saat Anda membuat model, Anda dapat mengaktifkan isolasi jaringan dengan mengatur nilai `EnableNetworkIsolation` parameter ke`True`.

[SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SageMaker::AppImageConfig`

AWS Config aturan: sagemaker-app-image-config-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah konfigurasi gambar aplikasi Amazon SageMaker AI (`AppImageConfig`) memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika konfigurasi gambar aplikasi tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya akan memeriksa keberadaan kunci tag dan gagal jika konfigurasi gambar aplikasi tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Mendefinisikan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna Sumber AWS Daya Tagging dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk menambahkan tag ke konfigurasi gambar aplikasi Amazon SageMaker AI (`AppImageConfig`), Anda dapat menggunakan pen AddTags goperasian API SageMaker AI atau, jika Anda menggunakan AWS CLI, jalankan perintah add-tags.

[SageMaker.7] SageMaker gambar harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SageMaker::Image`

AWS Config aturan: sagemaker-image-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Hub Keamanan
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi AWS persyaratan.	Tidak ada nilai default

Kontrol ini memeriksa apakah gambar Amazon SageMaker AI memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika gambar tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika gambar tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Mendefinisikan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna Sumber AWS Daya Tagging dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orang Layanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk menambahkan tag ke gambar Amazon SageMaker AI, Anda dapat menggunakan pen AddTags goperasian API SageMaker AI atau, jika Anda menggunakan AWS CLI, jalankan perintah add-tags.

[SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung

Kategori: Deteksi > Kerentanan, patch, dan manajemen versi

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: sagemaker-notebook-instance-platform-version

Jenis jadwal: Ber kala

Parameter:

- `supportedPlatformIdentifierVersions`: `notebook-al2023-v1` (tidak dapat disesuaikan)

Kontrol ini memeriksa apakah instance notebook Amazon SageMaker AI dikonfigurasi untuk berjalan pada platform yang didukung, berdasarkan pengidentifikasi platform yang ditentukan untuk instance notebook. Kontrol gagal jika instance notebook dikonfigurasi untuk berjalan pada platform yang tidak lagi didukung.

Jika platform untuk instance notebook Amazon SageMaker AI tidak lagi didukung, platform tersebut mungkin tidak menerima tambalan keamanan, perbaikan bug, atau jenis pembaruan lainnya. Instans notebook mungkin terus berfungsi, tetapi tidak akan menerima pembaruan keamanan SageMaker AI atau perbaikan bug penting. Anda menanggung risiko yang terkait dengan penggunaan platform yang tidak didukung. Untuk informasi selengkapnya, lihat JupyterLab pembuatan versi di Panduan Pengembang SageMaker AI Amazon.

Remediasi

Untuk informasi tentang platform yang saat ini didukung Amazon SageMaker AI dan cara bermigrasi ke platform tersebut, lihat instance notebook Amazon Linux 2 di Panduan Pengembang Amazon SageMaker AI.

[SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::DataQualityJobDefinition`

AWS Config aturan: sagemaker-data-quality-job-encrypt-in-transit

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan kualitas data Amazon SageMaker AI mengaktifkan enkripsi untuk lalu lintas antar kontainer. Kontrol gagal jika definisi untuk pekerjaan yang memantau kualitas dan penyimpangan data tidak mengaktifkan enkripsi untuk lalu lintas antar kontainer.

Mengaktifkan enkripsi lalu lintas antar kontainer melindungi data ML sensitif selama pemrosesan terdistribusi untuk analisis kualitas data.

Remediasi

Untuk informasi selengkapnya tentang enkripsi lalu lintas antar kontainer untuk Amazon SageMaker AI, lihat Mel indungi Komunikasi Antara Instans Komputasi ML dalam Pekerjaan Pelatihan Terdistribusi di Panduan Pengembang SageMaker AI Amazon. Saat Anda membuat definisi pekerjaan kualitas data, Anda dapat mengaktifkan enkripsi lalu lintas antar kontainer dengan menyetel nilai `EnableInterContainerTrafficEncryption` parameter ke`True`.

[SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::ModelExplainabilityJobDefinition`

AWS Config aturan: sagemaker-model-explainability-job-encrypt-in-transit

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan penjelasan SageMaker model Amazon mengaktifkan enkripsi lalu lintas antar kontainer. Kontrol gagal jika definisi pekerjaan penjelasan model tidak mengaktifkan enkripsi lalu lintas antar kontainer.

Mengaktifkan enkripsi lalu lintas antar kontainer melindungi data ML sensitif seperti data model, kumpulan data pelatihan, hasil pemrosesan menengah, parameter, dan bobot model selama pemrosesan terdistribusi untuk analisis keterjelasan.

Remediasi

Untuk definisi pekerjaan penjelasan SageMaker model yang ada, enkripsi lalu lintas antar kontainer tidak dapat diperbarui di tempat. Untuk membuat definisi pekerjaan penjelasan SageMaker model baru dengan enkripsi lalu lintas antar kontainer diaktifkan, gunakan API atau CLI atau CloudFormation dan setel ke. `EnableInterContainerTrafficEncryption` `True`

[SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::DataQualityJobDefinition`

AWS Config aturan: sagemaker-data-quality-job-isolation

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan pemantauan kualitas data Amazon SageMaker AI mengaktifkan isolasi jaringan. Kontrol gagal jika definisi untuk pekerjaan yang memantau kualitas data dan penyimpangan memiliki isolasi jaringan dinonaktifkan.

Isolasi jaringan mengurangi permukaan serangan dan mencegah akses eksternal sehingga melindungi terhadap akses eksternal yang tidak sah, paparan data yang tidak disengaja, dan potensi eksfiltrasi data.

Remediasi

Untuk informasi selengkapnya tentang isolasi jaringan untuk SageMaker AI, lihat Menjalankan wadah pelatihan dan inferensi dalam mode bebas internet di Panduan Pengembang SageMaker

AI Amazon. Saat Anda membuat definisi pekerjaan kualitas data, Anda dapat mengaktifkan isolasi jaringan dengan menyetel nilai `EnableNetworkIsolation` parameter ke`True`.

[SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan

Kategori: L indungi > Konfigurasi jaringan aman > Konfigurasi kebijakan sumber daya

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::ModelBiasJobDefinition`

AWS Config aturan: sagemaker-model-bias-job-isolation

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan bias SageMaker model mengaktifkan isolasi jaringan. Kontrol gagal jika definisi pekerjaan bias model tidak mengaktifkan isolasi jaringan.

Isolasi jaringan mencegah pekerjaan bias SageMaker model berkomunikasi dengan sumber daya eksternal melalui internet. Dengan mengaktifkan isolasi jaringan, Anda memastikan bahwa wadah pekerjaan tidak dapat membuat koneksi keluar, mengurangi permukaan serangan dan melindungi data sensitif dari eksfiltrasi. Ini sangat penting untuk pekerjaan yang memproses data yang diatur atau sensitif.

Remediasi

Untuk mengaktifkan isolasi jaringan, Anda harus membuat definisi pekerjaan bias model baru dengan `EnableNetworkIsolation` parameter disetel ke`True`. Isolasi jaringan tidak dapat dimodifikasi setelah pembuatan definisi pekerjaan. Untuk membuat definisi pekerjaan bias model baru, lihat CreateModelBiasJobDefinition di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::ModelQualityJobDefinition`

AWS Config aturan: ssagemaker-model-quality-job-encrypt-in-transit

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan kualitas SageMaker model Amazon mengaktifkan enkripsi dalam transit untuk lalu lintas antar kontainer. Kontrol gagal jika definisi pekerjaan kualitas model tidak mengaktifkan enkripsi lalu lintas antar kontainer.

Inter-container enkripsi lalu lintas melindungi data yang dikirimkan antar kontainer selama pekerjaan pemantauan kualitas model terdistribusi. Secara default, lalu lintas antar kontainer tidak dienkripsi. Mengaktifkan enkripsi membantu menjaga kerahasiaan data selama pemrosesan dan mendukung kepatuhan terhadap persyaratan peraturan untuk perlindungan data dalam transit.

Remediasi

Untuk mengaktifkan enkripsi lalu lintas antar kontainer untuk definisi pekerjaan kualitas SageMaker model Amazon Anda, Anda harus membuat ulang definisi pekerjaan dengan konfigurasi enkripsi dalam transit yang sesuai. Untuk membuat definisi pekerjaan berkualitas model, lihat CreateModelQualityJobDefinition di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan

Kategori: L indungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::MonitoringSchedule`

AWS Config aturan: sagemaker-monitoring-schedule-isolation

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah jadwal SageMaker pemantauan Amazon mengaktifkan isolasi jaringan. Kontrol gagal jika jadwal pemantauan telah diset EnableNetworkIsolation el ke false atau tidak dikonfigurasi

Isolasi jaringan mencegah pekerjaan pemantauan dari melakukan panggilan jaringan keluar, mengurangi permukaan serangan dengan menghilangkan akses internet dari kontainer.

Remediasi

Untuk informasi tentang mengonfigurasi isolasi jaringan dalam NetworkConfig parameter saat membuat atau memperbarui jadwal pemantauan, lihat CreateMonitoringSchedule atau UpdateMonitoringSchedule di Panduan Pengembang Amazon SageMaker AI.

[SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

Kategori: Mel indungi > Perlindungan Data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::ModelBiasJobDefinition`

AWS Config aturan: sagemaker-model-bias-job-encrypt-in-transit

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan bias SageMaker model Amazon mengaktifkan enkripsi lalu lintas antar kontainer saat menggunakan beberapa instans komputasi. Kontrol gagal jika `EnableInterContainerTrafficEncryption` disetel ke false atau tidak dikonfigurasi untuk definisi pekerjaan dengan jumlah instance 2 atau lebih besar.

Inter-container enkripsi lalu lintas melindungi data yang ditransmisikan antara instance komputasi selama pekerjaan pemantauan bias model terdistribusi. Enkripsi mencegah akses tidak sah ke informasi terkait model seperti bobot yang ditransmisikan antar instans.

Remediasi

Untuk mengaktifkan enkripsi lalu lintas antar kontainer untuk definisi pekerjaan bias SageMaker model, setel `EnableInterContainerTrafficEncryption` parameter ke `True` saat definisi pekerjaan menggunakan beberapa instance komputasi. Untuk informasi tentang melindungi komunikasi antara instans komputasi ML, lihat Mel indungi Komunikasi Antara Instans Komputasi ML dalam Pekerjaan Pelatihan Terdistribusi di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya dalam VPC

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::Model`

AWS Config aturan: sagemaker-model-private-registry-required

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah model Amazon SageMaker AI menarik gambar kontainer dari registri pribadi di VPC untuk wadah utama. Kontrol gagal jika gambar tidak dikonfigurasi atau mode akses repositori tidak`Platform`.

Menggunakan registri Docker pribadi di VPC untuk wadah SageMaker model memastikan gambar kontainer ditarik dari sumber tepercaya dan terkontrol dalam VPC Anda. Selain itu, ini memastikan gambar kontainer diakses melalui titik akhir VPC, tanpa melintasi internet publik.

Remediasi

Untuk mengonfigurasi registri docker pribadi untuk wadah inferensi real-time SageMaker AI, lihat Menggunakan Registry Docker Pribadi untuk Kontainer Real-Time Inferensi di Panduan Pengembang Amazon AI. SageMaker

[SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys

Kategori: Mel indungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::FeatureGroup`

AWS Config aturan: sagemaker-featuregroup-encryption-at-rest

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah toko SageMaker offline Amazon untuk grup fitur dienkripsi saat diam dengan AWS KMS kunci. Kontrol gagal jika penyimpanan S3 penyimpanan offline untuk grup fitur tidak dienkripsi dengan kunci KMS.

Menggunakan pengelolaan pelanggan AWS KMS keys untuk enkripsi di toko offline grup SageMaker fitur lainnya memberikan keamanan yang ditingkatkan. Customer-managed Kunci KMS memberi

Anda kontrol penuh atas siklus hidup kunci enkripsi dan kebijakan kunci. Selain itu, semua penggunaan kunci enkripsi dapat dicatat dan dipantau AWS CloudTrail untuk auditabilitas.

Remediasi

Untuk informasi tentang mengaktifkan enkripsi saat diam untuk toko offline Fe SageMaker ature Store menggunakan AWS KMS kunci yang dikelola pelanggan, lihat Keamanan dan kontrol akses di Panduan Pengembang Amazon SageMaker AI.

[SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys

Persyaratan terkait: NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Kategori: Melindungi > Perlindungan data > Enkripsi data saat diam

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::FeatureGroup`

AWS Config aturan: sagemaker-featuregroup-online-store-encryption

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah toko SageMaker online Amazon untuk grup fitur dengan penyimpanan standar dienkripsi saat diam dengan AWS KMS kunci. Kontrol gagal jika enkripsi kunci KMS tidak dikonfigurasi untuk toko online.

Menggunakan pengelolaan pelanggan AWS KMS keys untuk enkripsi di toko online grup SageMaker fitur lainnya memberikan keamanan yang ditingkatkan. Customer-managed Kunci KMS memberi Anda kontrol penuh atas siklus hidup kunci enkripsi dan kebijakan kunci. Selain itu, semua penggunaan kunci enkripsi dapat dicatat dan dipantau AWS CloudTrail untuk auditabilitas.

Remediasi

Untuk informasi tentang mengaktifkan enkripsi saat diam untuk toko online Fe SageMaker ature Store menggunakan AWS KMS kunci yang dikelola pelanggan, lihat Keamanan dan kontrol akses di Panduan Pengembang Amazon SageMaker AI.

[SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya dalam VPC

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::Model`

AWS Config aturan: sagemaker-model-multicontainer-private-registry

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah model Amazon SageMaker AI dengan pipeline inferensi multi-kontainer menarik gambar kontainer dari registri Docker pribadi di VPC. Kontrol gagal jika definisi wadah apa pun tidak memiliki konfigurasi gambar atau memiliki mode akses repositori diatur ke platform.

Menggunakan registri Docker pribadi di VPC untuk saluran inferensi multi-kontainer SageMaker AI memastikan gambar kontainer ditarik dari sumber tepercaya dan terkontrol dalam VPC Anda. Ini memastikan gambar kontainer diakses melalui titik akhir VPC, tanpa melintasi internet publik, mengurangi risiko serangan rantai pasokan atau gangguan gambar.

Remediasi

Untuk mengonfigurasi registri docker pribadi untuk wadah inferensi real-time SageMaker AI, lihat Menggunakan Registry Docker Pribadi untuk Kontainer Real-Time Inferensi di Panduan Pengembang Amazon AI. SageMaker

[SageMaker.20] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan isolasi jaringan

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::ModelExplainabilityJobDefinition`

AWS Config aturan: sagemaker-model-explainability-job-network-isolation

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan penjelasan model SageMaker AI mengaktifkan isolasi jaringan. Kontrol gagal jika definisi pekerjaan tidak mengaktifkan isolasi jaringan.

Isolasi jaringan mencegah wadah pekerjaan penjelasan model melakukan panggilan jaringan keluar, mengurangi risiko eksfiltrasi data dan memberikan pertahanan mendalam untuk model sensitif dan data pelatihan.

Remediasi

Untuk mengaktifkan isolasi jaringan untuk definisi pekerjaan penjelasan model SageMaker AI, setel `NetworkConfig.EnableNetworkIsolation` ke `true` saat membuat definisi pekerjaan. Untuk informasi selengkapnya tentang isolasi jaringan untuk SageMaker AI, lihat Menjalankan wadah pelatihan dan inferensi dalam mode bebas internet di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.21] instance SageMaker notebook harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys

Kategori: Melindungi > Perlindungan data > Enkripsi data saat diam

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::NotebookInstance`

AWS Config aturan: sagemaker-notebook-instance-storage-vol-kms-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instance notebook SageMaker AI dikonfigurasi dengan AWS KMS kunci untuk enkripsi volume penyimpanan. Kontrol gagal jika kunci KMS tidak dikonfigurasi untuk instance notebook.

Enkripsi data diam dengan kunci KMS yang dikelola pelanggan memberikan kontrol akses tambahan atas enkripsi terkel AWS ola default. SageMaker Instans notebook AI menyimpan buku catatan pengguna, kumpulan data, artefak model, dan data pemrosesan sementara pada volume penyimpanan ML. Kunci yang dikelola pelanggan memungkinkan kontrol kebijakan kunci yang

halus, pencatatan CloudTrail audit penggunaan kunci, dan kepatuhan terhadap kerangka kerja yang memerlukan enkripsi yang dikendalikan pelanggan.

Remediasi

Untuk mengonfigurasi kunci KMS untuk instance notebook SageMaker AI, lihat Instans Notebook, pekerjaan SageMaker AI, dan Titik Akhir di Panduan Pengembang SageMaker AI Amazon. Perhatikan bahwa hanya `KmsKeyId` dapat diatur pada waktu pembuatan instance notebook. Untuk memperbaiki, buat instance buku catatan baru dengan kunci KMS yang ditentukan dan migrasikan data Anda dari instance yang ada.

[SageMaker.22] jadwal SageMaker pemantauan harus mengaktifkan enkripsi lalu lintas antar kontainer

Kategori: Melindungi > Perlindungan data > Enkripsi data dalam transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::MonitoringSchedule`

AWS Config aturan: sagemaker-monitoring-schedule-traffic-encryption

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah jadwal pemantauan SageMaker AI Amazon mengaktifkan enkripsi untuk lalu lintas antar kontainer. Kontrol gagal jika definisi pekerjaan pemantauan tidak mengaktifkan enkripsi untuk lalu lintas antar kontainer.

Inter-container enkripsi lalu lintas memastikan bahwa data yang dikirimkan antar kontainer selama pekerjaan pemantauan dienkripsi saat transit. Tanpa enkripsi ini, data sensitif yang diproses selama pemantauan model dapat terkena akses tidak sah di dalam jaringan. Mengaktifkan pengaturan ini membantu memenuhi persyaratan kepatuhan untuk melindungi data dalam perjalanan.

Remediasi

Untuk jadwal pemantauan SageMaker AI yang ada, enkripsi lalu lintas antar kontainer tidak dapat diperbarui di tempat. Untuk membuat jadwal pemantauan SageMaker AI baru dengan enkripsi lalu lintas antar kontainer diaktifkan, gunakan API atau CLI atau CloudFormation

dan set `EnableInterContainerTrafficEncryption` el ke `true` dalam`NetworkConfig`. `MonitoringJobDefinition`

[SageMaker.23] eksperimen SageMaker inferensi harus memiliki volume penyimpanan instance yang dienkripsi dengan yang dikelola pelanggan AWS KMS keys

Kategori: Melindungi > Perlindungan data > Enkripsi data saat diam

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::InferenceExperiment`

AWS Config aturan: sagemaker-inf-experiment-instance-storage-kms-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah eksperimen inferensi SageMaker AI dikonfigurasi dengan AWS KMS kunci misalnya enkripsi volume penyimpanan. Kontrol gagal jika kunci KMS tidak ditentukan misalnya enkripsi volume penyimpanan.

Mengenkripsi volume penyimpanan instans dengan kunci KMS yang dikelola pelanggan menyediakan manajemen kunci terpusat, pencatatan audit, dan kontrol rotasi kunci untuk artefak model dan data inferensi sementara yang disimpan pada instans komputasi ML selama pengujian bayangan.

Remediasi

Untuk mengonfigurasi kunci KMS untuk eksperimen inferensi SageMaker AI, tentukan `KmsKey` parameter saat memanggil. `CreateInferenceExperiment` Bisa `KmsKey` berupa ID kunci KMS, ARN, alias, atau alias ARN. Per SageMaker an eksekusi AI harus memiliki `kms:CreateGrant` izin pada kunci. Untuk informasi selengkapnya tentang menentukan AWS KMS kunci yang dikelola pelanggan untuk SageMaker AI, lihat Inst ans Notebook, pekerjaan SageMaker AI, dan Titik Ak hir di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.24] eksperimen SageMaker inferensi harus memiliki penyimpanan data yang dienkripsi dengan pengelolaan pelanggan AWS KMS keys

Kategori: Melindungi > Perlindungan data > Enkripsi data saat diam

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SageMaker::InferenceExperiment`

AWS Config aturan: sagemaker-inf-experiment-data-storage-kms-encrypted

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah eksperimen inferensi SageMaker AI dengan pengambilan data diaktifkan memiliki kunci KMS yang dikonfigurasi untuk mengenkripsi data yang diambil saat diam. Kontrol gagal jika konfigurasi penyimpanan data tidak menentukan kunci KMS untuk enkripsi.

Mengenkripsi data permintaan inferensi dan respons yang ditangkap dengan kunci KMS yang dikelola pelanggan memastikan bahwa muatan inferensi sensitif yang disimpan di Amazon S3 dilindungi dengan kemampuan manajemen kunci dan audit terpusat.

Remediasi

Untuk mengonfigurasi kunci KMS untuk penyimpanan data dalam eksperimen inferensi SageMaker AI, tentukan `KmsKey` bidang di dalam `DataStorageConfig` saat memanggil. `CreateInferenceExperiment` Men `KmsKey` genkripsi permintaan inferensi yang ditangkap dan data respons saat diam di bucket Amazon S3 yang ditentukan. Untuk informasi selengkapnya tentang menentukan AWS KMS kunci yang dikelola pelanggan untuk SageMaker AI, lihat Inst ans Notebook, pekerjaan SageMaker AI, dan Titik Ak hir di Panduan Pengembang SageMaker AI Amazon.

[SageMaker.25] definisi pekerjaan kualitas SageMaker model harus mengaktifkan isolasi jaringan

Kategori: L indungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SageMaker::ModelQualityJobDefinition`

AWS Config aturan: sagemaker-model-quality-job-definition-isolation

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah definisi pekerjaan kualitas model Amazon SageMaker AI mengaktifkan isolasi jaringan. Kontrol gagal jika definisi pekerjaan kualitas model tidak mengaktifkan isolasi jaringan.

Isolasi jaringan mengurangi permukaan serangan dan mencegah akses eksternal, sehingga melindungi terhadap akses eksternal yang tidak sah, paparan data yang tidak disengaja, dan potensi eksfiltrasi data.

Remediasi

Saat Anda membuat definisi pekerjaan kualitas model, Anda dapat mengaktifkan isolasi jaringan dengan menyetel nilai `EnableNetworkIsolation` parameter ke`True`. Untuk informasi selengkapnya tentang isolasi jaringan untuk SageMaker AI, lihat Menjalankan wadah pelatihan dan inferensi dalam mode bebas internet di Panduan Pengembang SageMaker AI Amazon.

Kontrol CSPM Security Hub untuk Secrets Manager

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Secrets Manager layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/8.6.3, PCI DSS v4.0. 1/8.3.9

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Configaturan: **`secretsmanager-rotation-enabled-check`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`maximumAllowedRota`	Jumlah hari maksimum yang diizinkan untuk frekuensi rotasi rahasia	Bilangan Bulat	1 untuk 365	Tidak ada nilai default

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`tionFrequency`				

Kontrol ini memeriksa apakah rahasia yang disimpan AWS Secrets Manager dikonfigurasi dengan rotasi otomatis. Kontrol gagal jika rahasia tidak dikonfigurasi dengan rotasi otomatis. Jika Anda memberikan nilai khusus untuk `maximumAllowedRotationFrequency` parameter, kontrol hanya akan berlalu jika rahasia diputar secara otomatis dalam jendela waktu yang ditentukan.

Secrets Manager membantu Anda meningkatkan postur keamanan organisasi Anda. Rahasia mencakup kredensi basis data, kata sandi, dan kunci API pihak ketiga. Anda dapat menggunakan Secrets Manager untuk menyimpan rahasia secara terpusat, mengenkripsi rahasia secara otomatis, mengontrol akses ke rahasia, dan memutar rahasia dengan aman dan otomatis.

Secrets Manager dapat memutar rahasia. Anda dapat menggunakan rotasi untuk mengganti rahasia jangka panjang dengan rahasia jangka pendek. Memutar rahasia Anda membatasi berapa lama pengguna yang tidak sah dapat menggunakan rahasia yang disusupi. Untuk alasan ini, Anda harus sering memutar rahasia Anda. Untuk mempelajari lebih lanjut tentang rotasi, lihat Memutar AWS Secrets Manager rahasia Anda di Panduan AWS Secrets Manager Pengguna.

Remediasi

Untuk mengaktifkan rotasi otomatis rahasia Secrets Manager, lihat Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia menggunakan konsol di Panduan AWS Secrets Manager Pengguna. Anda harus memilih dan mengkonfigurasi AWS Lambda fungsi untuk rotasi.

[SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/8.6.3, PCI DSS v4.0. 1/8.3.9

Kategori: Lindungi > Pengembangan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Configaturan: **`secretsmanager-scheduled-rotation-success-check`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia berhasil diputar berdasarkan jadwal rotasi. Kontrol gagal jika `RotationOccurringAsScheduled` ada`false`. Kontrol hanya mengevaluasi rahasia yang telah dihidupkan rotasi.

Secrets Manager membantu Anda meningkatkan postur keamanan organisasi Anda. Rahasia mencakup kredensi basis data, kata sandi, dan kunci API pihak ketiga. Anda dapat menggunakan Secrets Manager untuk menyimpan rahasia secara terpusat, mengenkripsi rahasia secara otomatis, mengontrol akses ke rahasia, dan memutar rahasia dengan aman dan otomatis.

Secrets Manager dapat memutar rahasia. Anda dapat menggunakan rotasi untuk mengganti rahasia jangka panjang dengan rahasia jangka pendek. Memutar rahasia Anda membatasi berapa lama pengguna yang tidak sah dapat menggunakan rahasia yang disusupi. Untuk alasan ini, Anda harus sering memutar rahasia Anda.

Selain mengonfigurasi rahasia untuk berputar secara otomatis, Anda harus memastikan bahwa rahasia tersebut berhasil diputar berdasarkan jadwal rotasi.

Untuk mempelajari lebih lanjut tentang rotasi, lihat Memutar AWS Secrets Manager rahasia Anda di Panduan AWS Secrets Manager Pengguna.

Remediasi

Jika rotasi otomatis gagal, maka Secrets Manager mungkin mengalami kesalahan dengan konfigurasi. Untuk memutar rahasia di Secrets Manager, Anda menggunakan fungsi Lambda yang mendefinisikan cara berinteraksi dengan database atau layanan yang memiliki rahasia.

Untuk bantuan mendiagnosis dan memperbaiki kesalahan umum yang terkait dengan rotasi rahasia, lihat Memecahkan masalah AWS Secrets Manager rotasi rahasia di Panduan Pengguna. AWS Secrets Manager

[SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Configaturan: **`secretsmanager-secret-unused`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`unusedForDays`	Jumlah hari maksimum yang rahasia dapat tetap tidak digunakan	Bilangan Bulat	1 untuk 365	90

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia telah diakses dalam jangka waktu yang ditentukan. Kontrol gagal jika rahasia tidak digunakan di luar kerangka waktu yang ditentukan. Kecuali Anda memberikan nilai parameter khusus untuk periode akses, Security Hub CSPM menggunakan nilai default 90 hari.

Menghapus rahasia yang tidak digunakan sama pentingnya dengan memutar rahasia. Rahasia yang tidak digunakan dapat disalahgunakan oleh mantan pengguna mereka, yang tidak lagi membutuhkan akses ke rahasia ini. Selain itu, karena semakin banyak pengguna mendapatkan akses ke rahasia, seseorang mungkin salah menangani dan membocorkannya ke entitas yang tidak sah, yang meningkatkan risiko penyalahgunaan. Menghapus rahasia yang tidak digunakan membantu mencabut akses rahasia dari pengguna yang tidak lagi membutuhkannya. Ini juga membantu mengurangi biaya penggunaan Secrets Manager. Oleh karena itu, penting untuk secara rutin menghapus rahasia yang tidak digunakan.

Remediasi

Untuk menghapus rahasia Secrets Manager yang tidak aktif, lihat Menghapus AWS Secrets Manager rahasia di Panduan AWS Secrets Manager Pengguna.

[SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu

Persyaratan terkait: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), PCI DSS v4.0. 1/8.6.3, PCI DSS v4.0. 1/8.3.9

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Configaturan: **`secretsmanager-secret-periodic-rotation`**

Jenis jadwal: Periodik

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`maxDaysSinceRotation`	Jumlah hari maksimum yang rahasia dapat tetap tidak berubah	Bilangan Bulat	1 untuk `180`	`90`

Kontrol ini memeriksa apakah sebuah AWS Secrets Manager rahasia diputar setidaknya sekali dalam jangka waktu yang ditentukan. Kontrol gagal jika rahasia tidak diputar setidaknya ini sering. Kecuali Anda memberikan nilai parameter khusus untuk periode rotasi, Security Hub CSPM menggunakan nilai default 90 hari.

Rahasia berputar dapat membantu Anda mengurangi risiko penggunaan rahasia Anda yang tidak sah dalam diri Anda. Akun AWS Contohnya termasuk kredensi basis data, kata sandi, kunci API pihak ketiga, dan bahkan teks arbitrer. Jika Anda tidak mengubah rahasia Anda untuk jangka waktu yang lama, rahasianya lebih mungkin dikompromikan.

Karena semakin banyak pengguna mendapatkan akses ke rahasia, kemungkinan besar seseorang salah menangani dan membocorkannya ke entitas yang tidak sah. Rahasia dapat bocor melalui log dan data cache. Mereka dapat dibagikan untuk tujuan debugging dan tidak diubah atau dicabut setelah debugging selesai. Untuk semua alasan ini, rahasia harus sering diputar.

Anda dapat mengonfigurasi rotasi otomatis untuk rahasia diAWS Secrets Manager. Dengan rotasi otomatis, Anda dapat mengganti rahasia jangka panjang dengan rahasia jangka pendek, secara signifikan mengurangi risiko kompromi. Kami menyarankan Anda mengonfigurasi rotasi otomatis

untuk rahasia Secrets Manager Anda. Untuk informasi selengkapnya, lihat Memutar rahasia AWS Secrets Manager Anda di Panduan Pengguna AWS Secrets Manager.

Remediasi

Untuk mengaktifkan rotasi otomatis rahasia Secrets Manager, lihat Mengatur rotasi otomatis untuk AWS Secrets Manager rahasia menggunakan konsol di Panduan AWS Secrets Manager Pengguna. Anda harus memilih dan mengkonfigurasi AWS Lambda fungsi untuk rotasi.

[SecretsManager.5] Rahasia Secrets Manager harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SecretsManager::Secret`

AWS Configaturan: `tagged-secretsmanager-secret` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah AWS Secrets Manager rahasia memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika rahasia tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika rahasia tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke rahasia Secrets Manager, lihat Menandai AWS Secrets Manager rahasia di Panduan AWS Secrets Manager Pengguna.

Kontrol CSPM Security Hub untukAWS Service Catalog

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Service Catalog layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja

Persyaratan terkait: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

Kategori: Lindungi > Manajemen akses yang aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::ServiceCatalog::Portfolio`

AWS Configaturan: service-catalog-shared-within-organization

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Service Catalog berbagi portofolio dalam organisasi saat integrasi dengan AWS Organizations diaktifkan. Kontrol gagal jika portofolio tidak dibagikan dalam suatu organisasi.

Berbagi portofolio hanya dalam Organizations membantu memastikan bahwa portofolio tidak dibagikan dengan salahAkun AWS. Untuk berbagi portofolio Service Catalog dengan akun di suatu organisasi, Security Hub CSPM merekomendasikan penggunaan `ORGANIZATION_MEMBER_ACCOUNT` sebagai gantinya. `ACCOUNT` Ini menyederhanakan administrasi dengan mengatur akses yang diberikan ke akun di seluruh organisasi. Jika Anda memiliki kebutuhan bisnis untuk berbagi portofolio Service Catalog dengan akun eksternal, Anda dapat secara otomatis menekan temuan dari kontrol ini atau menonaktifkannya.

Remediasi

Untuk mengaktifkan berbagi portofolio denganAWS Organizations, lihat Berbagi dengan AWS Organizations di Panduan AWS Service Catalog Administrator.

Kontrol CSPM Security Hub untuk Amazon SES

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Email Service (Amazon SES).

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SES.1] Daftar kontak SES harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SES::ContactList`

AWS Configaturan: `tagged-ses-contactlist` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah daftar kontak Amazon SES memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika daftar kontak tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika daftar kontak tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke daftar kontak Amazon SES, lihat TagResourcedi Referensi Amazon SES API v2.

[SES.2] Set konfigurasi SES harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SES::ConfigurationSet`

AWS Configaturan: `tagged-ses-configurationset` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah set konfigurasi Amazon SES memiliki tag dengan kunci spesifik yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika set konfigurasi tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika set konfigurasi tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke set konfigurasi Amazon SES, lihat TagResourcedi Referensi Amazon SES API v2.

[SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SES::ConfigurationSet`

AWS Configaturan: ses-sending-tls-required

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah set konfigurasi Amazon SES memerlukan koneksi TLS. Kontrol gagal jika Kebijakan TLS tidak disetel ke `'REQUIRE'` set konfigurasi.

Secara default, Amazon SES menggunakan TLS oportunistik, yang berarti email dapat dikirim tanpa enkripsi jika koneksi TLS tidak dapat dibuat dengan server email penerima. Menegakkan TLS untuk pengiriman email memastikan bahwa pesan hanya terkirim ketika koneksi terenkripsi yang aman dapat dibuat. Ini membantu melindungi kerahasiaan dan integritas konten email selama transmisi antara Amazon SES dan server email penerima. Jika koneksi TLS aman tidak dapat dibuat, pesan tidak akan dikirimkan, mencegah potensi paparan informasi sensitif.

> **Note**
>
> Meskipun TLS 1.3 adalah metode pengiriman default untuk Amazon SES, tanpa menerapkan persyaratan TLS melalui set konfigurasi, pesan berpotensi dikirimkan dalam teks biasa jika koneksi TLS gagal. Untuk meneruskan kontrol ini, Anda harus mengonfigurasi Kebijakan TLS ke `'REQUIRE'` dalam opsi pengiriman set konfigurasi SES Anda. Ketika TLS diperlukan, pesan hanya dikirim jika koneksi TLS dapat dibuat dengan server email penerima.

Remediasi

Untuk mengonfigurasi Amazon SES agar memerlukan koneksi TLS untuk set konfigurasi, lihat Amazon SES dan protokol keamanan di Panduan Pengembang Amazon SES.

Kontrol CSPM Security Hub untuk Amazon SNS

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Notification Service (Amazon SNS). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SNS.1] Topik SNS harus dienkripsi saat istirahat menggunakanAWS KMS

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6),, NIST.800-53.r5 SC-13 NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6), NIST.800-171.r2 3.13.11, 3.13.16 NIST.800-171.r2

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SNS::Topic`

AWS Configaturan: **`sns-encrypted-kms`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah topik Amazon SNS dienkripsi saat istirahat menggunakan kunci yang dikelola di (). AWS Key Management Service AWS KMS Kontrol gagal jika topik SNS tidak menggunakan kunci KMS untuk enkripsi sisi server (SSE). Secara default, SNS menyimpan pesan dan file menggunakan enkripsi disk. Untuk melewati kontrol ini, Anda harus memilih untuk menggunakan kunci KMS untuk enkripsi sebagai gantinya. Ini menambahkan lapisan keamanan tambahan dan memberikan lebih banyak fleksibilitas kontrol akses.

Mengenkripsi data saat istirahat mengurangi risiko data yang disimpan pada disk diakses oleh pengguna yang tidak diautentikasi. AWS Izin API diperlukan untuk mendekripsi data sebelum dapat dibaca. Kami merekomendasikan mengenkripsi topik SNS dengan kunci KMS untuk lapisan keamanan tambahan.

Remediasi

Untuk mengaktifkan SSE untuk topik SNS, lihat Mengaktifkan enkripsi sisi server (SSE) untuk topik Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon. Sebelum Anda dapat menggunakan SSE, Anda juga harus mengonfigurasi AWS KMS key kebijakan untuk mengizinkan enkripsi topik dan enkripsi dan dekripsi pesan. Untuk informasi selengkapnya, lihat Mengonfigurasi AWS KMS izin di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.2] Pencatatan status pengiriman harus diaktifkan untuk pesan notifikasi yang dikirim ke suatu topik

> **Important**
>
> Security Hub CSPM menghentikan kontrol ini pada April 2024. Untuk informasi selengkapnya, lihat Log perubahan untuk kontrol CSPM Security Hub.

Persyaratan terkait: NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SNS::Topic`

AWS Configaturan: **`sns-topic-message-delivery-notification-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah pencatatan diaktifkan untuk status pengiriman pesan notifikasi yang dikirim ke topik Amazon SNS untuk titik akhir. Kontrol ini gagal jika pemberitahuan status pengiriman pesan tidak diaktifkan.

Logging adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja layanan. Mencatat status pengiriman pesan membantu memberikan wawasan operasional, seperti berikut ini:

- Mengetahui apakah pesan dikirim ke titik akhir Amazon SNS.
- Mengidentifikasi respon yang dikirim dari titik akhir Amazon SNS ke Amazon SNS.
- Menentukan waktu tinggal pesan (waktu antara stempel waktu publikasi dan penyerahan ke titik akhir Amazon SNS).

Remediasi

Untuk mengonfigurasi pencatatan status pengiriman untuk suatu topik, lihat Status pengiriman pesan Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.3] Topik SNS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SNS::Topic`

AWS Configaturan: `tagged-sns-topic` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah topik Amazon SNS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika topik tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika topik tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke topik SNS, lihat Mengonfigurasi tag topik Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

[SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::SNS::Topic`

AWS Configaturan: sns-topic-no-public-access

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan akses topik Amazon SNS memungkinkan akses publik. Kontrol ini gagal jika kebijakan akses topik SNS mengizinkan akses publik.

Anda menggunakan kebijakan akses Amazon SNS dengan topik tertentu untuk membatasi siapa yang dapat bekerja dengan topik tersebut (misalnya, siapa yang dapat mempublikasikan pesan ke topik tersebut atau siapa yang dapat berlangganan). Kebijakan SNS dapat memberikan akses ke orang lainAkun AWS, atau ke pengguna di dalam milik Akun AWS Anda. Menyediakan wildcard (*) di `Principal` bidang kebijakan topik dan kurangnya kondisi untuk membatasi kebijakan topik dapat mengakibatkan eksfiltrasi data, penolakan layanan, atau injeksi pesan yang tidak diinginkan ke layanan Anda oleh penyerang.

> **Note**
>
> Kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan `PASSED` temuan, kondisi dalam kebijakan akses Amazon SNS untuk suatu topik hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak berisi karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat Variabel dan tag di Panduan AWS Identity and Access Management Pengguna.

Remediasi

Untuk memperbarui kebijakan akses untuk topik SNS, lihat Ikhtisar mengelola akses di Amazon SNS di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

Kontrol CSPM Security Hub untuk Amazon SQS

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya Amazon Simple Queue Service (Amazon SQS). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6) NIST.800-53.r5 SC-13,, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Kategori: Lindungi > Perlindungan Data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::SQS::Queue`

AWS Configaturan: `sqs-queue-encrypted` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah antrian Amazon SQS dienkripsi saat istirahat. Kontrol gagal jika antrian tidak dienkripsi dengan SQS-managed key (SSE-SQS) atau () key AWS Key Management Service (AWS KMS). SSE-KMS

Mengenkripsi data saat istirahat mengurangi risiko pengguna yang tidak sah mengakses data yang disimpan di disk. Server-side enkripsi (SSE) melindungi isi pesan dalam antrian SQS menggunakan kunci SQS-managed enkripsi (SSE-SQS) atau AWS KMS kunci (). SSE-KMS

Remediasi

Untuk mengonfigurasi SSE untuk antrean SQS, lihat Mengonfigurasi enkripsi sisi server (SSE) untuk antrian (konsol) di Panduan Pengembang Layanan Antrian Sederhana Amazon.

[SQS.2] Antrian SQS harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SQS::Queue`

AWS Configaturan: `tagged-sqs-queue` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah antrian Amazon SQS memiliki tag dengan kunci tertentu yang ditentukan dalam parameter. `requiredTagKeys` Kontrol gagal jika antrian tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika antrian tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau

peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke antrean yang ada menggunakan konsol Amazon SQS, lihat Mengonfigurasi tag alokasi biaya untuk antrean (konsol) Amazon SQS di Panduan Pengembang Layanan Antrian Sederhana Amazon.

[SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::SQS::Queue`

AWS Configaturan: sqs-queue-no-public-access

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kebijakan akses Amazon SQS memungkinkan akses publik ke antrean SQS. Kontrol gagal jika kebijakan akses SQS mengizinkan akses publik ke antrian.

Kebijakan akses Amazon SQS dapat mengizinkan akses publik ke antrean SQS, yang memungkinkan pengguna anonim atau identitas AWS IAM yang diautentikasi untuk mengakses antrian. Kebijakan akses SQS biasanya menyediakan akses ini dengan menentukan karakter wildcard (`*`) dalam `Principal` elemen kebijakan, tidak menggunakan kondisi yang tepat untuk

membatasi akses ke antrian, atau keduanya. Jika kebijakan akses SQS mengizinkan akses publik, pihak ketiga mungkin dapat melakukan tugas seperti menerima pesan dari antrian, mengirim pesan ke antrian, atau mengubah kebijakan akses untuk antrian. Hal ini dapat mengakibatkan peristiwa seperti eksfiltrasi data, penolakan layanan, atau injeksi pesan ke dalam antrian oleh aktor ancaman.

> **Note**
>
> Kontrol ini tidak mengevaluasi kondisi kebijakan yang menggunakan karakter atau variabel wildcard. Untuk menghasilkan `PASSED` temuan, kondisi dalam kebijakan akses Amazon SQS untuk antrian hanya boleh menggunakan nilai tetap, yaitu nilai yang tidak berisi karakter wildcard atau variabel kebijakan. Untuk informasi tentang variabel kebijakan, lihat Variabel dan tag di Panduan AWS Identity and Access Management Pengguna.

Remediasi

Untuk informasi tentang mengonfigurasi kebijakan akses SQS untuk antrean SQS, lihat Menggunakan kebijakan khusus dengan Bahasa Kebijakan Akses Amazon SQS di Panduan Pengembang Layanan Antrian Sederhana Amazon.

Kontrol CSPM Security Hub untuk Step Functions

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Step Functions layanan dan sumber daya.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging

Persyaratan terkait: PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::StepFunctions::StateMachine`

AWS Configaturan: **`step-functions-state-machine-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`logLevel`	Tingkat logging minimum	Enum	`ALL`, `ERROR`, `FATAL`	Tidak ada nilai default

Kontrol ini memeriksa apakah mesin AWS Step Functions status telah mengaktifkan logging. Kontrol gagal jika mesin status tidak mengaktifkan logging. Jika Anda memberikan nilai khusus untuk `logLevel` parameter, kontrol hanya akan diteruskan jika mesin status mengaktifkan level logging yang ditentukan.

Pemantauan membantu Anda menjaga keandalan, ketersediaan, dan kinerja Step Functions. Anda harus mengumpulkan sebanyak mungkin data pemantauan dari Layanan AWS yang Anda gunakan sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik. Memiliki konfigurasi logging yang ditentukan untuk mesin status Step Functions memungkinkan Anda melacak riwayat eksekusi dan hasil di Amazon CloudWatch Logs. Secara opsional, Anda hanya dapat melacak kesalahan atau peristiwa fatal.

Remediasi

Untuk mengaktifkan logging untuk mesin status Step Functions, lihat Mengkonfigurasi logging di Panduan AWS Step Functions Pengembang.

[StepFunctions.2] Aktivitas Step Functions harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::StepFunctions::Activity`

AWS Configaturan: `tagged-stepfunctions-activity` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Step Functions aktivitas memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika aktivitas tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika aktivitas tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke aktivitas Step Functions, lihat Menandai di Step Functions di Panduan AWS Step Functions Pengembang.

Kontrol CSPM Security Hub untuk Systems Manager

AWS Security Hub CSPMKontrol ini mengevaluasi layanan dan sumber daya AWS Systems Manager (SSM). Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[SSM.1] Instans Amazon EC2 harus dikelola olehAWS Systems Manager

Persyaratan terkait: PCI DSS v3.2. 1/2.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SA-15 (2), NIST.800-53.r5 SA-15 (8), NIST.800-53.r5 SA-3, NIST.800-53.r5 SI-2 (3)

Kategori: Identifikasi > Persediaan

Tingkat keparahan: Sedang

Sumber daya yang dievaluasi: `AWS::EC2::Instance`

Sumber daya AWS Config perekaman yang diperlukan:`AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

AWS Configaturan: ec2-instance-managed-by-systems-manager

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah instans EC2 yang berhenti dan berjalan di akun Anda dikelola oleh. AWS Systems Manager Systems Manager adalah Layanan AWS yang dapat Anda gunakan untuk melihat dan mengontrol AWS infrastruktur Anda.

Untuk membantu Anda menjaga keamanan dan kepatuhan, Systems Manager memindai instans terkelola yang berhenti dan berjalan. Sebuah instance terkelola adalah mesin yang dikonfigurasi untuk digunakan dengan Systems Manager. Systems Manager kemudian melaporkan atau mengambil tindakan korektif atas setiap pelanggaran kebijakan yang terdeteksi. Systems Manager

juga membantu Anda mengkonfigurasi dan mempertahankan instans terkelola Anda. Untuk mempelajari selengkapnya, lihat Panduan Pengguna AWS Systems Manager.

> **Note**
>
> Kontrol ini menghasilkan `FAILED` temuan untuk instans EC2 yang merupakan instance Server AWS Elastic Disaster Recovery Replikasi yang dikelola oleh. AWS Instance Server Replikasi adalah Instans EC2 yang diluncurkan secara otomatis AWS Elastic Disaster Recovery untuk mendukung replikasi data berkelanjutan dari server sumber. AWSSengaja menghapus Agen Systems Manager (SSM) dari instans ini untuk menjaga isolasi dan membantu mencegah potensi jalur akses yang tidak diinginkan.

Remediasi

Untuk informasi tentang mengelola instans EC2 denganAWS Systems Manager, lihat manajemen host Amazon EC2 di AWS Systems Manager Panduan Pengguna. Di bagian Opsi konfigurasi di AWS Systems Manager konsol, Anda dapat menyimpan pengaturan default atau mengubahnya seperlunya untuk konfigurasi pilihan Anda.

[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch

Persyaratan terkait: NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (3), (4), NIST.800-53.r5 SI-2 NIST.800-53.r5 SI-2 (5), NIST.800-171.r2 3.7.1, PCI DSS v3.2. 1/6.2, PCI DSS v4.0. 1/2.2.1, PCI DSS v4.0. 1/6.3.3

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Tinggi

Jenis sumber daya: `AWS::SSM::PatchCompliance`

AWS Configaturan: ec2-managedinstance-patch-compliance-status-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah status kepatuhan kepatuhan patch Systems Manager `COMPLIANT` atau `NON_COMPLIANT` setelah instalasi patch pada instance. Kontrol gagal jika status

kepatuhan`NON_COMPLIANT`. Kontrol hanya memeriksa instance yang dikelola oleh Systems Manager Patch Manager.

Menambal instans EC2 Anda seperti yang dipersyaratkan oleh organisasi Anda mengurangi permukaan serangan Anda. Akun AWS

Remediasi

Systems Manager merekomendasikan penggunaan kebijakan tambalan untuk mengonfigurasi patching untuk instance terkelola Anda. Anda juga dapat menggunakan dokumen Systems Manager, seperti yang dijelaskan dalam prosedur berikut, untuk menambal instance.

Untuk memulihkan tambalan yang tidak sesuai

1. Buka AWS Systems Manager konsol di https://console.aws.amazon.com/systems-manager/.
2. Untuk Node Management, pilih Run Command, dan kemudian pilih Run command.
3. Pilih opsi untuk AWS- RunPatchBaseline.
4. Ubah Operasi untuk Menginstal.
5. Pilih instans secara manual, lalu pilih instans yang tidak sesuai.
6. Pilih Jalankan.
7. Setelah perintah selesai, untuk memantau status kepatuhan baru dari instance yang ditambal, pilih Kepatuhan di panel navigasi.

[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2 (3), PCI DSS v3.2. 1/2.4, PCI DSS v4.0. 1/2.2.1, PCI DSS v4.0. 1/6.3.3

Kategori: Deteksi > Layanan deteksi

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SSM::AssociationCompliance`

AWS Configaturan: ec2-managedinstance-association-compliance-status-check

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah status kepatuhan AWS Systems Manager asosiasi `COMPLIANT` atau `NON_COMPLIANT` setelah asosiasi dijalankan pada sebuah instance. Kontrol gagal jika status kepatuhan asosiasi`NON_COMPLIANT`.

Asosiasi State Manager adalah konfigurasi yang ditetapkan untuk instans terkelola Anda. Konfigurasi mendefinisikan status yang ingin Anda pertahankan pada instans Anda. Misalnya, asosiasi dapat menentukan bahwa perangkat lunak antivirus harus diinstal dan berjalan pada instance Anda atau port tertentu harus ditutup.

Setelah Anda membuat satu atau beberapa asosiasi Manajer Negara, informasi status kepatuhan segera tersedia untuk Anda. Anda dapat melihat status kepatuhan di konsol atau sebagai respons terhadap AWS CLI perintah atau tindakan API Systems Manager terkait. Untuk asosiasi, Kepatuhan Konfigurasi menunjukkan status kepatuhan (`Compliant`atau`Non-compliant`). Ini juga menunjukkan tingkat keparahan yang ditetapkan untuk asosiasi, seperti `Critical` atau`Medium`.

Untuk mempelajari lebih lanjut tentang kepatuhan asosiasi Manajer Negara, lihat Tentang kepatuhan asosiasi Manajer Negara di Panduan AWS Systems Manager Pengguna.

Remediasi

Asosiasi yang gagal dapat dikaitkan dengan hal-hal yang berbeda, termasuk target dan nama dokumen Systems Manager. Untuk mengatasi masalah ini, Anda harus terlebih dahulu mengidentifikasi dan menyelidiki asosiasi dengan melihat riwayat asosiasi. Untuk petunjuk tentang melihat riwayat asosiasi, lihat Melihat riwayat asosiasi di Panduan AWS Systems Manager Pengguna.

Setelah menyelidiki, Anda dapat mengedit asosiasi untuk memperbaiki masalah yang diidentifikasi. Anda dapat mengedit asosiasi untuk menentukan nama, jadwal, tingkat keparahan, atau target baru. Setelah Anda mengedit asosiasi, AWS Systems Manager buat versi baru. Untuk petunjuk tentang mengedit asosiasi, lihat Mengedit dan membuat versi baru asosiasi di Panduan AWS Systems Manager Pengguna.

[SSM.4] Dokumen SSM seharusnya tidak bersifat publik

Persyaratan terkait: NIST.800-53.r5 AC-21 NIST.800-53.r5 AC-3,, NIST.800-53.r5 AC-3 (7) NIST.800-53.r5 AC-4,, NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Kategori: Lindungi > Konfigurasi jaringan aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::SSM::Document`

AWS Configaturan: ssm-document-not-public

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Systems Manager dokumen yang dimiliki oleh akun bersifat publik. Kontrol gagal jika dokumen Systems Manager yang memiliki `Self` sebagai pemilik bersifat publik.

Dokumen Systems Manager yang bersifat publik mungkin memungkinkan akses yang tidak diinginkan ke dokumen Anda. Dokumen Systems Manager publik dapat mengekspos informasi berharga tentang akun, sumber daya, dan proses internal Anda.

Kecuali kasus penggunaan Anda memerlukan berbagi publik, sebaiknya Anda memblokir berbagi publik untuk dokumen Systems Manager yang dimiliki `Self` sebagai pemiliknya.

Remediasi

Untuk informasi tentang mengonfigurasi berbagi untuk dokumen Systems Manager, lihat Membagikan dokumen SSM di AWS Systems ManagerPanduan Pengguna.

[SSM.5] Dokumen SSM harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::SSM::Document`

AWS Configaturan: ssm-document-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Systems Manager dokumen memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika dokumen tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika dokumen tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan. Kontrol tidak mengevaluasi dokumen Systems Manager yang dimiliki oleh Amazon.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk menambahkan tag ke AWS Systems Manager dokumen, Anda dapat menggunakan AddTagsToResourcepengoperasian AWS Systems Manager API atau, jika Anda menggunakanAWS CLI, jalankan perintah add-tags-to-resource. Anda juga dapat menggunakan AWS Systems Manager konsol.

[SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: ssm-automation-logging-enabled

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudWatch pencatatan Amazon diaktifkan untuk Otomasi AWS Systems Manager (SSM). Kontrol gagal jika CloudWatch logging tidak diaktifkan untuk SSM Automation.

SSM Automation adalah AWS Systems Manager alat yang membantu Anda membangun solusi otomatis untuk menyebarkan, mengonfigurasi, dan mengelola AWS sumber daya dalam skala besar menggunakan runbook yang telah ditentukan atau kustom. Untuk memenuhi persyaratan operasional atau keamanan untuk organisasi Anda, Anda mungkin perlu memberikan catatan skrip yang dijalankannya. Anda dapat mengonfigurasi SSM Automation untuk mengirim output dari `aws:executeScript` tindakan di runbook ke grup CloudWatch log Amazon Logs yang Anda tentukan. Dengan CloudWatch Log, Anda dapat memantau, menyimpan, dan mengakses file log dari berbagai fileLayanan AWS.

Remediasi

Untuk informasi tentang mengaktifkan CloudWatch logging untuk Otomasi SSM, lihat Keluaran tindakan Otomasi Pencatatan dengan CloudWatch Log di AWS Systems ManagerPanduan Pengguna.

[SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik

Kategori: Lindungi > Manajemen akses aman > Sumber daya tidak dapat diakses publik

Tingkat keparahan: Kritis

Jenis sumber daya: `AWS::::Account`

AWS Configaturan: ssm-automation-block-public-sharing

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah setelan blok berbagi publik diaktifkan untuk AWS Systems Manager dokumen. Kontrol gagal jika setelan blok berbagi publik dinonaktifkan untuk dokumen Systems Manager.

Pengaturan blok berbagi publik untuk dokumen AWS Systems Manager (SSM) adalah pengaturan tingkat akun. Mengaktifkan pengaturan ini dapat mencegah akses yang tidak diinginkan ke dokumen SSM Anda. Jika Anda mengaktifkan setelan ini, perubahan Anda tidak memengaruhi dokumen SSM apa pun yang saat ini Anda bagikan dengan publik. Kecuali kasus penggunaan Anda mengharuskan Anda untuk berbagi dokumen SSM dengan publik, kami sarankan Anda mengaktifkan pengaturan blokir berbagi publik. Pengaturan dapat berbeda untuk masing-masingWilayah AWS.

Remediasi

Untuk informasi tentang mengaktifkan setelan blokir berbagi publik untuk dokumen AWS Systems Manager (SSM), lihat Memblokir berbagi publik untuk dokumen SSM di Panduan Pengguna. AWS Systems Manager

Kontrol CSPM Security Hub untukAWS Transfer Family

AWS Security Hub CSPMKontrol ini mengevaluasi AWS Transfer Family layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[Transfer.1]AWS Transfer Familyalur kerja harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Workflow`

AWS Configaturan: `tagged-transfer-workflow` (aturan CSPM Security Hub kustom)

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredTagKeys`	Daftar kunci tag non-sistem yang harus berisi sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	`No default value`

Kontrol ini memeriksa apakah AWS Transfer Family alur kerja memiliki tag dengan kunci tertentu yang ditentukan dalam parameter`requiredTagKeys`. Kontrol gagal jika alur kerja tidak memiliki kunci tag atau jika tidak memiliki semua kunci yang ditentukan dalam parameter`requiredTagKeys`. Jika parameter `requiredTagKeys` tidak disediakan, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika alur kerja tidak ditandai dengan kunci apa pun. Tag sistem, yang secara otomatis diterapkan dan dimulai dengan`aws:`, diabaikan.

Tag adalah label yang Anda tetapkan ke AWS sumber daya, dan itu terdiri dari kunci dan nilai opsional. Anda dapat menggunakan tanda untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Tag dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Penandaan juga membantu Anda melacak pemilik sumber daya yang bertanggung jawab untuk tindakan dan pemberitahuan. Saat menggunakan penandaan, Anda dapat menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi, yang menentukan izin berdasarkan tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke AWS sumber daya. Anda dapat membuat kebijakan ABAC tunggal atau serangkaian kebijakan terpisah untuk prinsipal IAM Anda. Anda dapat mendesain kebijakan ABAC ini untuk mengizinkan operasi saat tag prinsipal cocok dengan tag sumber daya. Untuk informasi lebih lanjut, lihat Untuk apa ABAC? AWS di Panduan Pengguna IAM.

> **Note**
>
> Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak orangLayanan AWS, termasukAWS

Billing. Untuk praktik terbaik penandaan lainnya, lihat Menandai AWS sumber daya Anda di. Referensi Umum AWS

Remediasi

Untuk menambahkan tag ke alur kerja Transfer Family (konsol)

1. Buka AWS Transfer Family konsol.
2. Di panel navigasi, pilih Alur Kerja. Kemudian, pilih alur kerja yang ingin Anda tag.
3. Pilih Kelola tag, lalu tambahkan tag.

[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir

Persyaratan terkait: NIST.800-53.r5 CM-7,, NIST.800-53.r5 IA-5 NIST.800-53.r5 SC-8, PCI DSS v4.0.1/4.2.1

Kategori: Lindungi > Perlindungan Data > Enkripsi data-in-transit

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Transfer::Server`

AWS Configaturan: transfer-family-server-no-ftp

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS Transfer Family server menggunakan protokol selain FTP untuk koneksi endpoint. Kontrol gagal jika server menggunakan protokol FTP untuk klien untuk terhubung ke endpoint server.

FTP (File Transfer Protocol) menetapkan koneksi titik akhir melalui saluran yang tidak terenkripsi, meninggalkan data yang dikirim melalui saluran ini rentan terhadap intersepsi. Menggunakan SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure), atau AS2 (Applicability Statement 2) menawarkan lapisan keamanan ekstra dengan mengenkripsi data Anda dalam perjalanan dan dapat digunakan untuk membantu mencegah penyerang potensial menggunakan serangan orang di tengah atau serupa untuk menguping atau memanipulasi lalu lintas jaringan.

Remediasi

Untuk mengubah protokol server Transfer Family, lihat Mengedit protokol transfer file di AWS Transfer FamilyPanduan Pengguna.

[Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging

Persyaratan terkait: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9) NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8)

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::Transfer::Connector`

AWS Configaturan: transfer-connector-logging-enabled

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah CloudWatch pencatatan Amazon diaktifkan untuk AWS Transfer Family konektor. Kontrol gagal jika CloudWatch logging tidak diaktifkan untuk konektor.

Amazon CloudWatch adalah layanan pemantauan dan observabilitas yang memberikan visibilitas ke AWS sumber daya Anda, termasuk AWS Transfer Family sumber daya. Untuk Transfer Family, CloudWatch menyediakan audit dan pencatatan terkonsolidasi untuk kemajuan dan hasil alur kerja. Ini mencakup beberapa metrik yang didefinisikan Transfer Family untuk alur kerja. Anda dapat mengonfigurasi Transfer Family untuk secara otomatis mencatat peristiwa konektor CloudWatch. Untuk melakukan ini, Anda menentukan peran logging untuk konektor. Untuk peran logging, Anda membuat peran IAM dan kebijakan IAM berbasis sumber daya yang menentukan izin untuk peran tersebut.

Remediasi

Untuk informasi tentang mengaktifkan CloudWatch logging untuk konektor Transfer Family, lihat Amazon CloudWatch logging untuk AWS Transfer Family server di Panduan AWS Transfer Family Pengguna.

[Transfer.4] Perjanjian Transfer Family harus ditandai

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Agreement`

AWS Configaturan: transfer-agreement-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Transfer Family perjanjian memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika perjanjian tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika perjanjian tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan

atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family perjanjian, lihat Metode penandaan sumber daya di Panduan Pengguna AWS Sumber Daya Tag dan Editor Tag.

[Transfer.5] Sertifikat Transfer Family harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Certificate`

AWS Configaturan: transfer-certificate-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Transfer Family sertifikat memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika sertifikat tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika sertifikat tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family sertifikat, lihat Metode penandaan sumber daya di Panduan Pengguna AWS Sumber Daya Tag dan Editor Tag.

[Transfer.6] Konektor Transfer Family harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Connector`

AWS Configaturan: transfer-connector-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Transfer Family konektor memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika konektor tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika konektor tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family konektor, lihat Metode penandaan sumber daya di Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

[Transfer.7] Profil Transfer Family harus diberi tag

Kategori: Identifikasi > Inventaris > Penandaan

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::Transfer::Profile`

AWS Configaturan: transfer-profile-tagged

Jenis jadwal: Perubahan dipicu

Parameter:

Parameter	Deskripsi	Tipe	Nilai kustom yang diizinkan	Nilai default CSPM Security Hub
`requiredKeyTags`	Daftar kunci tag non-sistem yang harus ditetapkan ke sumber daya yang dievaluasi. Kunci tag peka huruf besar dan kecil.	StringList (maksimal 6 item)	1—6 kunci tag yang memenuhi persyaratanAWS.	Tidak ada nilai default

Kontrol ini memeriksa apakah AWS Transfer Family profil memiliki kunci tag yang ditentukan oleh `requiredKeyTags` parameter. Kontrol gagal jika profil tidak memiliki kunci tag, atau tidak memiliki semua kunci yang ditentukan oleh `requiredKeyTags` parameter. Jika Anda tidak menentukan nilai apa pun untuk `requiredKeyTags` parameter, kontrol hanya memeriksa keberadaan kunci tag dan gagal jika profil tidak memiliki kunci tag. Kontrol mengabaikan tag sistem, yang diterapkan secara otomatis dan memiliki `aws:` awalan. Kontrol mengevaluasi profil lokal dan profil mitra.

Tag adalah label yang Anda buat dan tetapkan ke AWS sumber daya. Setiap tanda terdiri dari kunci tanda yang diperlukan dan nilai tanda opsional. Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Mereka dapat membantu

Anda mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Mereka juga dapat membantu Anda melacak pemilik sumber daya untuk tindakan dan pemberitahuan. Anda juga dapat menggunakan tag untuk menerapkan kontrol akses berbasis atribut (ABAC) sebagai strategi otorisasi. Untuk informasi selengkapnya tentang strategi ABAC, lihat Menentukan izin berdasarkan atribut dengan otorisasi ABAC di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang tag, lihat Panduan Pengguna AWS Sumber Daya Penandaan dan Editor Tag.

> **Note**
>
> Jangan menyimpan informasi pengenal pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS. Mereka tidak dimaksudkan untuk digunakan untuk data pribadi atau sensitif.

Remediasi

Untuk informasi tentang menambahkan tag ke AWS Transfer Family profil, lihat Metode penandaan sumber daya di Panduan Pengguna AWS Sumber Daya Tag dan Editor Tag.

Kontrol CSPM Security Hub untukAWS WAF

AWS Security Hub CSPMKontrol ini mengevaluasi AWS WAF layanan dan sumber daya. Kontrol mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::WebACL`

AWS Configaturan: **`waf-classic-logging-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk ACL web AWS WAF global. Kontrol ini gagal jika logging tidak diaktifkan untuk ACL web.

Logging adalah bagian penting untuk menjaga keandalan, ketersediaan, dan kinerja AWS WAF global. Ini adalah persyaratan bisnis dan kepatuhan di banyak organisasi, dan memungkinkan Anda memecahkan masalah perilaku aplikasi. Ini juga memberikan informasi rinci tentang lalu lintas yang dianalisis oleh ACL web yang dilampirkanAWS WAF.

Remediasi

Untuk mengaktifkan pencatatan untuk ACL AWS WAF web, lihat Mencatat informasi lalu lintas ACL web di Panduan AWS WAFPengembang.

[WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat

Persyaratan terkait: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::Rule`

AWS Configaturan: **`waf-regional-rule-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah aturan AWS WAF Regional memiliki setidaknya satu syarat. Kontrol gagal jika tidak ada kondisi dalam suatu aturan.

Aturan Regional WAF dapat berisi beberapa kondisi. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa kondisi apa pun, lalu lintas berlalu tanpa inspeksi. Aturan Regional WAF tanpa kondisi, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk menambahkan kondisi ke aturan kosong, lihat Menambahkan dan menghapus kondisi dalam aturan di Panduan AWS WAF Pengembang.

[WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan

Persyaratan terkait: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::RuleGroup`

AWS Configaturan: **`waf-regional-rulegroup-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah kelompok aturan AWS WAF Regional memiliki setidaknya satu aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan Regional WAF dapat berisi beberapa aturan. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa aturan apa pun, lalu lintas berlalu tanpa inspeksi. Kelompok aturan Regional WAF tanpa aturan, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk menambahkan aturan dan ketentuan aturan ke grup aturan kosong, lihat Menambahkan dan menghapus aturan dari grup aturan AWS WAF Klasik serta Menambahkan dan menghapus kondisi dalam aturan di Panduan AWS WAF Pengembang.

[WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFRegional::WebACL`

AWS Configaturan: **`waf-regional-webacl-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ACL AWS WAF Classic Regional web berisi aturan WAF atau grup aturan WAF. Kontrol ini gagal jika ACL web tidak berisi aturan WAF atau grup aturan.

ACL web Regional WAF dapat berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengontrol permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF tergantung pada tindakan default.

Remediasi

Untuk menambahkan aturan atau grup aturan ke ACL web Regional AWS WAF Klasik kosong, lihat Mengedit ACL Web di Panduan AWS WAF Pengembang.

[WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::Rule`

AWS Configaturan: **`waf-global-rule-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah aturan AWS WAF global berisi kondisi apa pun. Kontrol gagal jika tidak ada kondisi dalam suatu aturan.

Aturan global WAF dapat berisi beberapa kondisi. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa kondisi apa pun, lalu lintas berlalu tanpa inspeksi. Aturan global WAF tanpa kondisi, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk petunjuk cara membuat aturan dan menambahkan kondisi, lihat Membuat aturan dan menambahkan kondisi di Panduan AWS WAF Pengembang.

[WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::RuleGroup`

AWS Configaturan: **`waf-global-rulegroup-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah grup aturan AWS WAF global memiliki setidaknya satu aturan. Kontrol gagal jika tidak ada aturan dalam kelompok aturan.

Grup aturan global WAF dapat berisi beberapa aturan. Ketentuan aturan memungkinkan inspeksi lalu lintas dan mengambil tindakan yang ditentukan (izinkan, blokir, atau hitung). Tanpa aturan apa pun, lalu lintas berlalu tanpa inspeksi. Grup aturan global WAF tanpa aturan, tetapi dengan nama atau tag yang menyarankan izinkan, blokir, atau hitung, dapat menyebabkan asumsi yang salah bahwa salah satu tindakan tersebut terjadi.

Remediasi

Untuk petunjuk cara menambahkan aturan ke grup aturan, lihat Membuat grup aturan AWS WAF Klasik di Panduan AWS WAF Pengembang.

[WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Persyaratan terkait: NIST.800-53.r5 AC-4 (21) NIST.800-53.r5 SC-7,, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAF::WebACL`

AWS Configaturan: **`waf-global-webacl-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah ACL web AWS WAF global berisi setidaknya satu aturan WAF atau grup aturan WAF. Kontrol gagal jika ACL web tidak berisi aturan WAF atau grup aturan.

ACL web global WAF dapat berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengontrol permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti oleh WAF tergantung pada tindakan default.

Remediasi

Untuk menambahkan aturan atau grup aturan ke ACL web AWS WAF global yang kosong, lihat Mengedit ACL web di Panduan AWS WAF Pengembang. Untuk Filter, pilih Global (CloudFront).

[WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan

Persyaratan terkait: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Kategori: Lindungi > Konfigurasi jaringan aman

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFv2::WebACL`

AWS Configaturan: **`wafv2-webacl-not-empty`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah daftar kontrol akses web AWS WAF V2 (web ACL) berisi setidaknya satu aturan atau grup aturan. Kontrol gagal jika ACL web tidak berisi aturan atau grup aturan apa pun.

ACL web memberi Anda kontrol halus atas semua permintaan web HTTP (S) yang ditanggapi oleh sumber daya Anda yang dilindungi. ACL web harus berisi kumpulan aturan dan kelompok aturan yang memeriksa dan mengontrol permintaan web. Jika ACL web kosong, lalu lintas web dapat lewat tanpa terdeteksi atau ditindaklanjuti dengan AWS WAF tergantung pada tindakan default.

Remediasi

Untuk menambahkan aturan atau grup aturan ke ACL web WAFV2 kosong, lihat Mengedit ACL Web di Panduan Pengembang. AWS WAF

[WAF.11]AWS WAFpencatatan ACL web harus diaktifkan

Persyaratan terkait: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-7 (8), PCI DSS v4.0. 1/10.4.2

Kategori: Identifikasi > Logging

Tingkat keparahan: Rendah

Jenis sumber daya: `AWS::WAFv2::WebACL`

AWS Configaturan: **`wafv2-logging-enabled`**

Jenis jadwal: Periodik

Parameter: Tidak ada

Kontrol ini memeriksa apakah logging diaktifkan untuk daftar kontrol akses web AWS WAF V2 (web ACL). Kontrol ini gagal jika logging dinonaktifkan untuk ACL web.

> **Note**
>
> Kontrol ini tidak memeriksa apakah pencatatan ACL AWS WAF web diaktifkan untuk akun melalui Amazon Security Lake.

Logging mempertahankan keandalan, ketersediaan, dan kinerjaAWS WAF. Selain itu, penebangan adalah persyaratan bisnis dan kepatuhan di banyak organisasi. Dengan mencatat lalu lintas yang dianalisis oleh ACL web Anda, Anda dapat memecahkan masalah perilaku aplikasi.

Remediasi

Untuk mengaktifkan logging untuk ACL AWS WAF web, lihat Mengelola logging untuk ACL web di Panduan AWS WAF Pengembang.

[WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik

Persyaratan terkait: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (10), (9), NIST.800-53.r5 SC-7 NIST.800-53.r5 SI-7 (8), NIST.800-171.r2 3.14.6, 3.14.7 NIST.800-171.r2

Kategori: Identifikasi > Logging

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WAFv2::RuleGroup`

AWS Configaturan: **`wafv2-rulegroup-logging-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah AWS WAF aturan atau grup aturan mengaktifkan CloudWatch metrik Amazon. Kontrol gagal jika aturan atau grup aturan tidak mengaktifkan CloudWatch metrik.

Mengkonfigurasi CloudWatch metrik pada AWS WAF aturan dan grup aturan memberikan visibilitas ke arus lalu lintas. Anda dapat melihat aturan ACL mana yang dipicu dan permintaan mana yang diterima dan diblokir. Visibilitas ini dapat membantu Anda mengidentifikasi aktivitas berbahaya pada sumber daya terkait.

Remediasi

Untuk mengaktifkan CloudWatch metrik pada grup AWS WAF aturan, panggil API. UpdateRuleGroup Untuk mengaktifkan CloudWatch metrik pada AWS WAF aturan, panggil

UpdateWebACL API. Atur `CloudWatchMetricsEnabled` bidang `ketrue`. Saat Anda menggunakan AWS WAF konsol untuk membuat aturan atau grup aturan, CloudWatch metrik diaktifkan secara otomatis.

Kontrol CSPM Security Hub untuk WorkSpaces

AWS Security Hub CSPMKontrol ini mengevaluasi WorkSpaces layanan dan sumber daya Amazon.

Kontrol ini mungkin tidak tersedia di semuaWilayah AWS. Untuk informasi selengkapnya, lihat Ketersediaan kontrol berdasarkan Wilayah.

[WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WorkSpaces::Workspace`

AWS Configaturan: **`workspaces-user-volume-encryption-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah volume pengguna di Amazon WorkSpaces WorkSpace dienkripsi saat istirahat. Kontrol gagal jika volume WorkSpace pengguna tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengenkripsi volume WorkSpaces pengguna, lihat Mengenkripsi WorkSpace di Panduan WorkSpaces Administrasi Amazon.

[WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Kategori: Lindungi > Perlindungan data > Enkripsi data-at-rest

Tingkat keparahan: Sedang

Jenis sumber daya: `AWS::WorkSpaces::Workspace`

AWS Configaturan: **`workspaces-root-volume-encryption-enabled`**

Jenis jadwal: Perubahan dipicu

Parameter: Tidak ada

Kontrol ini memeriksa apakah volume root di Amazon WorkSpaces WorkSpace dienkripsi saat istirahat. Kontrol gagal jika volume WorkSpace root tidak dienkripsi saat istirahat.

Data saat istirahat mengacu pada data yang disimpan dalam penyimpanan persisten dan tidak mudah menguap untuk durasi berapa pun. Mengenkripsi data saat istirahat membantu Anda melindungi kerahasiaannya, yang mengurangi risiko bahwa pengguna yang tidak sah dapat mengaksesnya.

Remediasi

Untuk mengenkripsi volume WorkSpaces root, lihat Mengenkripsi a WorkSpace di Panduan WorkSpaces Administrasi Amazon.

Izin yang diperlukan untuk mengonfigurasi kontrol di Security Hub CSPM

Untuk melihat informasi tentang kontrol keamanan dan mengaktifkan serta menonaktifkan kontrol keamanan dalam standar, peran AWS Identity and Access Management (IAM) yang Anda gunakan untuk mengakses CSPM AWS Security Hub memerlukan izin untuk memanggil operasi CSPM API Security Hub berikut ini.

Untuk mendapatkan izin yang diperlukan, Anda dapat menggunakan kebijakan terkelola CSPM Security Hub. Atau, Anda dapat memperbarui kebijakan IAM khusus untuk menyertakan izin untuk tindakan ini.

- BatchGetSecurityControls— Mengembalikan informasi tentang sekumpulan kontrol keamanan untuk akun saat ini danWilayah AWS.
- ListSecurityControlDefinitions— Mengembalikan informasi tentang kontrol keamanan yang berlaku untuk standar tertentu.
- ListStandardsControlAssociations— Mengidentifikasi apakah kontrol keamanan saat ini diaktifkan atau dinonaktifkan dari setiap standar yang diaktifkan di akun.

- BatchGetStandardsControlAssociations— Untuk sekumpulan kontrol keamanan, identifikasi apakah setiap kontrol saat ini diaktifkan atau dinonaktifkan dari standar yang ditentukan.
- BatchUpdateStandardsControlAssociationsDigunakan untuk mengaktifkan kontrol keamanan dalam standar yang mencakup kontrol, atau untuk menonaktifkan kontrol dalam standar. Ini adalah pengganti batch untuk `UpdateStandardsControl`operasi yang ada.
- BatchUpdateStandardsControlAssociations— Digunakan untuk mengaktifkan atau menonaktifkan sekumpulan kontrol keamanan dalam standar yang mencakup kontrol. Ini adalah pengganti batch untuk `UpdateStandardsControl`operasi yang ada.
- UpdateStandardsControl— Digunakan untuk mengaktifkan atau menonaktifkan kontrol keamanan tunggal dalam standar yang mencakup kontrol
- DescribeStandardsControl— Mengembalikan rincian tentang kontrol keamanan tertentu.

Selain API sebelumnya, Anda harus menambahkan izin untuk memanggil `BatchGetControlEvaluations` ke peran IAM Anda. Izin ini diperlukan untuk melihat status pemberdayaan dan kepatuhan kontrol, jumlah temuan untuk kontrol, dan skor keamanan keseluruhan untuk kontrol pada konsol CSPM Security Hub. Karena hanya panggilan konsol`BatchGetControlEvaluations`, izin ini tidak secara langsung sesuai dengan API atau perintah CSPM Security Hub yang didokumentasikan secara publik. AWS CLI

Mengaktifkan kontrol di Security Hub CSPM

Dalam AWS Security Hub CSPM, kontrol adalah perlindungan dalam standar keamanan yang membantu organisasi melindungi kerahasiaan, integritas, dan ketersediaan informasinya. Setiap kontrol CSPM Security Hub terkait dengan sumber daya tertentu AWS . Saat Anda mengaktifkan kontrol, Security Hub CSPM mulai menjalankan pemeriksaan keamanan untuk kontrol dan menghasilkan temuan untuk kontrol tersebut. Security Hub CSPM juga mempertimbangkan semua kontrol yang diaktifkan saat menghitung skor keamanan.

Anda dapat memilih untuk mengaktifkan kontrol di semua standar keamanan yang berlaku. Atau, Anda dapat mengonfigurasi status pengaktifan secara berbeda dalam standar yang berbeda. Kami merekomendasikan opsi sebelumnya, di mana status pengaktifan kontrol diselaraskan di semua standar yang diaktifkan. Untuk petunjuk tentang mengaktifkan kontrol di semua standar yang menerapkannya, lihatMengaktifkan kontrol lintas standar. Untuk petunjuk tentang mengaktifkan kontrol dalam standar tertentu, lihatMengaktifkan kontrol dalam standar tertentu.

Jika Anda mengaktifkan agregasi lintas wilayah dan masuk ke Wilayah agregasi, konsol CSPM Hub Keamanan menampilkan kontrol yang tersedia di setidaknya satu Wilayah tertaut. Jika kontrol

tersedia di Wilayah tertaut tetapi tidak di Wilayah agregasi, Anda tidak dapat mengaktifkan atau menonaktifkan kontrol itu dari Wilayah agregasi.

Anda dapat mengaktifkan dan menonaktifkan kontrol di setiap Wilayah dengan menggunakan konsol CSPM Security Hub, Security Hub CSPM API, atau. AWS CLI

Petunjuk untuk mengaktifkan dan menonaktifkan kontrol bervariasi berdasarkan apakah Anda menggunakan konfigurasi pusat atau tidak. Topik ini menjelaskan perbedaannya. Konfigurasi pusat tersedia untuk pengguna yang mengintegrasikan Security Hub CSPM dan. AWS Organizations Sebaiknya gunakan konfigurasi pusat untuk menyederhanakan proses mengaktifkan dan menonaktifkan kontrol di lingkungan multi-akun, Multi-wilayah. Jika Anda menggunakan konfigurasi pusat, Anda dapat mengaktifkan kontrol di beberapa akun dan Wilayah melalui penggunaan kebijakan konfigurasi. Jika Anda tidak menggunakan konfigurasi pusat, Anda harus mengaktifkan kontrol secara terpisah di setiap Wilayah dan akun.

Mengaktifkan kontrol lintas standar

Sebaiknya aktifkan kontrol CSPM Hub AWS Keamanan di semua standar yang berlaku untuk kontrol tersebut. Jika Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan kontrol meskipun kontrol termasuk dalam lebih dari satu standar.

Cross-standard pengaktifan di lingkungan multi-akun, Multi-wilayah

Untuk mengaktifkan kontrol keamanan di beberapa Akun AWS dan Wilayah AWS, Anda harus masuk ke akun administrator CSPM Hub Keamanan yang didelegasikan dan menggunakan konfigurasi pusat.

Di bawah konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang mengaktifkan kontrol tertentu di seluruh standar yang diaktifkan. Anda kemudian dapat mengaitkan kebijakan konfigurasi dengan akun tertentu dan unit organisasi (OU) atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan penyesuaian. Misalnya, Anda dapat memilih untuk mengaktifkan semua kontrol dalam satu OU, dan Anda dapat memilih untuk mengaktifkan hanya kontrol Amazon Elastic Compute Cloud (EC2) di OU lain. Tingkat perincian tergantung pada tujuan yang Anda inginkan untuk cakupan keamanan di organisasi Anda. Untuk petunjuk tentang membuat kebijakan konfigurasi yang mengaktifkan kontrol tertentu di seluruh standar, lihatMembuat dan mengaitkan kebijakan konfigurasi.

> **Note**
>
> Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengelola kontrol di semua standar kecuali Service-Managed Standar: AWS Control Tower. Kontrol untuk standar ini harus dikonfigurasi dalam AWS Control Tower layanan.

Jika Anda ingin beberapa akun mengonfigurasi kontrol mereka sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai pengelola sendiri. Self-managed akun harus mengkonfigurasi kontrol secara terpisah di setiap Wilayah.

Cross-standard pengaktifan dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau merupakan akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk mengaktifkan kontrol secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menggunakan langkah-langkah berikut untuk mengaktifkan kontrol dalam satu akun dan Wilayah.

Security Hub CSPM console

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Kontrol dari panel navigasi.
3. Pilih tab Din onaktifkan.
4. Pilih opsi di sebelah kontrol.
5. Pilih Aktif kan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah diaktifkan).
6. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

Security Hub CSPM API

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Memanggil ListStandardsControlAssociations API. Berikan ID kontrol keamanan.

   Contoh permintaan:

```
{
```

```
    "SecurityControlId": "IAM.1"
}
```

2. Memanggil BatchUpdateStandardsControlAssociations API. Berikan Nama Sumber Daya Amazon (ARN) dari setiap standar yang tidak diaktifkan kontrolnya. Untuk mendapatkan ARN standar, jalankan `DescribeStandards`.
3. Atur `AssociationStatus` parameter sama dengan`ENABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, API mengembalikan respons kode status HTTP 200.

   Contoh permintaan:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]
}
```

4. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

AWS CLI

Untuk mengaktifkan kontrol lintas standar dalam satu akun dan Wilayah

1. Jalankan perintah list-standards-control-associations. Berikan ID kontrol keamanan.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Jalankan perintah batch-update-standards-control-associations. Berikan Nama Sumber Daya Amazon (ARN) dari setiap standar yang tidak diaktifkan kontrolnya. Untuk mendapatkan ARN standar, jalankan `describe-standards` perintah.
3. Atur `AssociationStatus` parameter sama dengan`ENABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, perintah mengembalikan respons kode status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
```

```
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Ulangi di setiap Wilayah di mana Anda ingin mengaktifkan kontrol.

Mengaktifkan kontrol dalam standar tertentu

Saat Anda mengaktifkan standar di AWS Security Hub CSPM, semua kontrol yang berlaku untuk standar tersebut secara otomatis diaktifkan dalam standar tersebut (pengecualian untuk ini adalah standar yang dikelola layanan). Anda kemudian dapat menonaktifkan dan mengaktifkan kembali kontrol tertentu dalam standar. Namun, sebaiknya selaraskan status pengaktifan kontrol di semua standar yang diaktifkan. Untuk petunjuk tentang mengaktifkan kontrol di semua standar, lihatMengaktifkan kontrol lintas standar.

Halaman detail untuk standar berisi daftar kontrol yang berlaku untuk standar, dan informasi tentang kontrol mana yang saat ini diaktifkan dan dinonaktifkan di standar tersebut.

Pada halaman detail standar, Anda juga dapat mengaktifkan kontrol dalam standar tertentu. Anda harus mengaktifkan kontrol dalam standar tertentu secara terpisah di masing-masing Akun AWS dan Wilayah AWS. Bila Anda mengaktifkan kontrol dalam standar tertentu, itu hanya memengaruhi akun saat ini dan Wilayah.

Untuk mengaktifkan kontrol dalam standar, Anda harus terlebih dahulu mengaktifkan setidaknya satu standar yang diterapkan kontrol. Untuk petunjuk tentang mengaktifkan standar, lihatMengaktifkan standar keamanan. Saat Anda mengaktifkan kontrol dalam satu atau beberapa standar, Security Hub CSPM mulai menghasilkan temuan untuk kontrol tersebut. Security Hub CSPM menyertakan status kontrol dalam perhitungan skor keamanan keseluruhan dan skor keamanan standar. Bahkan jika Anda mengaktifkan kontrol dalam beberapa standar, Anda akan menerima satu temuan per pemeriksaan keamanan di seluruh standar jika Anda mengaktifkan temuan kontrol konsolidasi. Untuk informasi selengkapnya, lihat Temuan kontrol konsolidasi.

Untuk mengaktifkan kontrol dalam standar, kontrol harus tersedia di Wilayah Anda saat ini. Untuk informasi selengkapnya, lihat Ketersediaan kontrol menurut Wilayah.

Ikuti langkah-langkah berikut untuk mengaktifkan kontrol CSPM Security Hub dalam standar tertentu. Sebagai pengganti langkah-langkah berikut, Anda juga dapat menggunakan tindakan

UpdateStandardsControl API untuk mengaktifkan kontrol dalam standar tertentu. Untuk petunjuk tentang mengaktifkan kontrol di semua standar, lihatCross-standard pengaktifan dalam satu akun dan Wilayah.

Security Hub CSPM console

Untuk mengaktifkan kontrol dalam standar tertentu

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Standar keamanan dari panel navigasi.
3. Pilih Lihat hasil untuk standar yang relevan.
4. Pilih kontrol.
5. Pilih Aktif kan Kontrol (opsi ini tidak muncul untuk kontrol yang sudah diaktifkan). Konfirmasikan dengan memilih Aktifkan.

Security Hub CSPM API

Untuk mengaktifkan kontrol dalam standar tertentu

1. J ListSecurityControlDefinitions alankan, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan DescribeStandards. API ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

   Contoh permintaan:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. J ListStandardsControlAssociations alankan, dan berikan ID kontrol tertentu untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

   Contoh permintaan:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. Jalankan BatchUpdateStandardsControlAssociations. Berikan ARN standar yang ingin Anda aktifkan kontrol.
4. Atur `AssociationStatus` parameter sama dengan`ENABLED`.

   Contoh permintaan:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Untuk mengaktifkan kontrol dalam standar tertentu

1. Jalan list-security-control-definitions kan perintah, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN standar, jalankan`describe-standards`. Perintah ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Jalan list-standards-control-associations kan perintah, dan berikan ID kontrol tertentu untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Jalankan perintah batch-update-standards-control-associations. Berikan ARN standar yang ingin Anda aktifkan kontrol.
4. Atur `AssociationStatus` parameter sama dengan`ENABLED`.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Mengaktifkan kontrol baru dalam standar yang diaktifkan secara otomatis

AWSSecurity Hub CSPM secara teratur merilis kontrol baru dan menambahkannya ke satu atau lebih standar. Anda dapat memilih apakah akan mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan.

Sebaiknya gunakan konfigurasi pusat CSPM Security Hub untuk mengaktifkan kontrol keamanan baru secara otomatis. Anda dapat membuat kebijakan konfigurasi yang menyertakan daftar kontrol yang akan dinonaktifkan di seluruh standar. Semua kontrol lainnya, termasuk yang baru dirilis, diaktifkan secara default. Atau, Anda dapat membuat kebijakan yang menyertakan daftar kontrol yang akan diaktifkan di seluruh standar. Semua kontrol lainnya, termasuk yang baru dirilis, dinonaktifkan secara default. Untuk informasi selengkapnya, lihat Memahami konfigurasi pusat di Security Hub CSPM.

Security Hub CSPM tidak mengaktifkan kontrol baru saat ditambahkan ke standar yang belum Anda aktifkan.

Petunjuk berikut hanya berlaku jika Anda tidak menggunakan konfigurasi pusat.

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah untuk mengaktifkan kontrol baru secara otomatis dalam standar yang diaktifkan.

> **Note**
>
> Saat Anda mengaktifkan kontrol baru secara otomatis menggunakan petunjuk berikut, Anda dapat berinteraksi dengan kontrol di konsol dan secara terprogram segera setelah rilis. Namun, kontrol yang diaktifkan secara otomatis memiliki status default sementara Dinonaktifkan. Diperlukan waktu hingga beberapa hari untuk Security Hub CSPM untuk memproses rilis kontrol dan menetapkan kontrol sebagai Diaktifkan di akun Anda. Selama periode pemrosesan, Anda dapat mengaktifkan atau menonaktifkan kontrol secara manual, dan Security Hub CSPM akan mempertahankan penunjukan itu terlepas dari apakah Anda mengaktifkan kontrol otomatis diaktifkan.

Security Hub CSPM console

Untuk mengaktifkan kontrol baru secara otomatis

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Pengaturan, lalu pilih tab Umum.
3. Di bawah Kontrol, pilih Edit.
4. Aktifkan kontrol Auto-enable baru dalam standar yang diaktifkan.
5. Pilih Simpan.

Security Hub CSPM API

Untuk mengaktifkan kontrol baru secara otomatis

1. Jalankan `UpdateSecurityHubConfiguration`.
2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, setel `AutoEnableControls` ke`true`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, setel `AutoEnableControls` ke false.

AWS CLI

Untuk mengaktifkan kontrol baru secara otomatis

1. Jalankan perintah `update-security-hub-configuration`.
2. Untuk mengaktifkan kontrol baru secara otomatis untuk standar yang diaktifkan, tentukan`--auto-enable-controls`. Jika Anda tidak ingin mengaktifkan kontrol baru secara otomatis, tentukan`--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Contoh perintah

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Jika Anda tidak secara otomatis mengaktifkan kontrol baru, maka Anda harus mengaktifkannya secara manual. Untuk petunjuk, lihat Mengaktifkan kontrol di Security Hub CSPM.

Menonaktifkan kontrol di Security Hub CSPM

Untuk mengurangi kebisingan pencarian, akan sangat membantu untuk menonaktifkan kontrol yang tidak relevan dengan lingkungan Anda. Di AWS Security Hub CSPM, Anda dapat menonaktifkan kontrol di semua standar keamanan atau hanya untuk standar tertentu.

Jika Anda menonaktifkan kontrol di semua standar, hal berikut terjadi:

- Pemeriksaan keamanan untuk kontrol tidak lagi dilakukan.
- Tidak ada temuan tambahan yang dihasilkan untuk kontrol.
- Temuan yang ada tidak lagi diperbarui untuk kontrol.
- Temuan yang ada untuk kontrol diarsipkan secara otomatis, biasanya dalam 3-5 hari berdasarkan upaya terbaik.
- Security Hub CSPM menghapus AWS Config aturan terkait yang dibuat untuk kontrol.

Jika Anda menonaktifkan kontrol hanya untuk standar tertentu, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan untuk kontrol hanya untuk standar tersebut. Ini juga menghapus kontrol dari perhitungan skor keamanan untuk masing-masing standar tersebut. Jika kontrol diaktifkan di standar lain, Security Hub CSPM mempertahankan AWS Config aturan terkait, jika berlaku, dan terus menjalankan pemeriksaan keamanan untuk kontrol untuk standar lainnya. Security Hub CSPM juga menyertakan kontrol saat menghitung skor keamanan untuk masing-masing standar lainnya, yang memengaruhi skor keamanan ringkasan Anda.

Jika Anda menonaktifkan standar, semua kontrol yang berlaku untuk standar dinonaktifkan secara otomatis untuk standar tersebut. Namun, kontrol mungkin terus diaktifkan di standar lain. Saat Anda menonaktifkan standar, Security Hub CSPM tidak melacak kontrol mana yang dinonaktifkan untuk standar tersebut. Akibatnya, jika nanti Anda mengaktifkan kembali standar yang sama, semua kontrol yang berlaku untuk itu secara otomatis diaktifkan. Untuk informasi tentang menonaktifkan standar, lihatMenonaktifkan standar.

Menonaktifkan kontrol bukanlah tindakan permanen. Misalkan Anda menonaktifkan kontrol, dan kemudian mengaktifkan standar yang menyertakan kontrol. Kontrol kemudian diaktifkan untuk standar itu. Saat Anda mengaktifkan standar di Security Hub CSPM, semua kontrol yang berlaku untuk standar secara otomatis diaktifkan. Untuk informasi tentang mengaktifkan standar, lihatMengaktifkan standar.

Topik

- Menonaktifkan kontrol di seluruh standar
- Menonaktifkan kontrol dalam standar tertentu
- Kontrol yang disarankan untuk dinonaktifkan di CSPM Security Hub

Menonaktifkan kontrol di seluruh standar

Sebaiknya nonaktifkan kontrol CSPM AWS Security Hub di seluruh standar untuk menjaga keselarasan di seluruh organisasi Anda. Jika Anda menonaktifkan kontrol hanya dalam standar tertentu, Anda akan terus menerima temuan untuk kontrol jika diaktifkan di standar lain.

Cross-standard penonaktifan di beberapa akun dan Wilayah

Untuk menonaktifkan kontrol keamanan di beberapa Akun AWS dan Wilayah AWS, Anda harus menggunakan konfigurasi pusat.

Saat Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi CSPM Security Hub yang menonaktifkan kontrol tertentu di seluruh standar yang diaktifkan. Anda kemudian dapat mengaitkan kebijakan konfigurasi dengan akun tertentu, OU, atau root. Kebijakan konfigurasi berlaku di Wilayah asal Anda (juga disebut Wilayah agregasi) dan semua Wilayah yang ditautkan.

Kebijakan konfigurasi menawarkan penyesuaian. Misalnya, Anda dapat memilih untuk menonaktifkan semua AWS CloudTrail kontrol dalam satu OU, dan Anda dapat memilih untuk menonaktifkan semua kontrol IAM di OU lain. Tingkat perincian tergantung pada tujuan yang Anda inginkan untuk cakupan keamanan di organisasi Anda. Untuk petunjuk tentang membuat kebijakan konfigurasi yang menonaktifkan kontrol tertentu di seluruh standar, lihatMembuat dan mengaitkan kebijakan konfigurasi.

> **Note**
>
> Administrator yang didelegasikan dapat membuat kebijakan konfigurasi untuk mengelola kontrol di semua standar kecuali Service-Managed Standar: AWS Control Tower. Kontrol untuk standar ini harus dikonfigurasi dalam AWS Control Tower layanan.

Jika Anda ingin beberapa akun mengonfigurasi kontrol mereka sendiri daripada administrator yang didelegasikan, administrator yang didelegasikan dapat menetapkan akun tersebut sebagai pengelola sendiri. Self-managed akun harus mengkonfigurasi kontrol secara terpisah di setiap Wilayah.

Cross-standard penonaktifan dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau merupakan akun yang dikelola sendiri, Anda tidak dapat menggunakan kebijakan konfigurasi untuk menonaktifkan kontrol secara terpusat di beberapa akun dan Wilayah. Namun, Anda dapat menonaktifkan kontrol dalam satu akun dan Wilayah.

Security Hub CSPM console

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Kontrol dari panel navigasi.
3. Pilih opsi di sebelah kontrol.
4. Pilih N onaktifkan Kontrol. Opsi ini tidak muncul untuk kontrol yang sudah dinonaktifkan.
5. Pilih alasan untuk menonaktifkan kontrol, dan konfirmasikan dengan memilih Non aktifkan.
6. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

Security Hub CSPM API

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Memanggil ListStandardsControlAssociations API. Berikan ID kontrol keamanan.

   Contoh permintaan:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. Memanggil BatchUpdateStandardsControlAssociations API. Berikan ARN standar apa pun di mana kontrol diaktifkan. Untuk mendapatkan ARN standar, jalankan `DescribeStandards`.
3. Atur `AssociationStatus` parameter sama dengan`DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, API mengembalikan respons kode status HTTP 200.

Contoh permintaan:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-
benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
 applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
 "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/
v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}}]
}
```

4. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

AWS CLI

Untuk menonaktifkan kontrol di seluruh standar dalam satu akun dan Wilayah

1. Jalankan perintah list-standards-control-associations. Berikan ID kontrol keamanan.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Jalankan perintah batch-update-standards-control-associations. Berikan ARN standar apa pun di mana kontrol diaktifkan. Untuk mendapatkan ARN standar, jalankan `describe-standards` perintah.
3. Atur `AssociationStatus` parameter sama dengan`DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, perintah mengembalikan respons kode status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-associations
 --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
 to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
 "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/v/1.4.0",
 "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
 environment"}]'
```

4. Ulangi di setiap Wilayah di mana Anda ingin menonaktifkan kontrol.

Menonaktifkan kontrol dalam standar tertentu

Anda dapat menonaktifkan kontrol hanya dalam standar keamanan tertentu, bukan di semua standar. Jika kontrol berlaku untuk standar lain yang diaktifkan, AWS Security Hub CSPM terus menjalankan pemeriksaan keamanan untuk kontrol dan Anda terus menerima temuan untuk kontrol tersebut.

Sebaiknya selaraskan status pengaktifan kontrol di semua standar yang diaktifkan yang diterapkan kontrol. Untuk informasi tentang menonaktifkan kontrol di semua standar yang berlaku, lihatMenonaktifkan kontrol di seluruh standar.

Pada halaman detail standar, Anda juga dapat menonaktifkan kontrol dalam standar tertentu. Anda harus menonaktifkan kontrol dalam standar tertentu secara terpisah di masing-masing Akun AWS dan Wilayah AWS. Ketika Anda menonaktifkan kontrol dalam standar tertentu, itu hanya memengaruhi akun saat ini dan Wilayah.

Pilih metode pilihan Anda, dan ikuti langkah-langkah ini untuk menonaktifkan kontrol dalam satu atau beberapa standar tertentu.

Security Hub CSPM console

Untuk menonaktifkan kontrol dalam standar tertentu

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Standar keamanan dari panel navigasi. Pilih Lihat hasil untuk standar yang relevan.
3. Pilih kontrol.
4. Pilih N onaktifkan Kontrol. Opsi ini tidak muncul untuk kontrol yang sudah dinonaktifkan.
5. Berikan alasan untuk menonaktifkan kontrol, dan konfirmasikan dengan memilih N onaktifkan.

Security Hub CSPM API

Untuk menonaktifkan kontrol dalam standar tertentu

1. J `ListSecurityControlDefinitions` alankan, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan ARN

standar, jalankan DescribeStandards. API ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

Contoh permintaan:

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. J ListStandardsControlAssociations alankan, dan berikan ID kontrol tertentu untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

   Contoh permintaan:

```
{
    "SecurityControlId": "IAM.1"
}
```

3. Jalankan BatchUpdateStandardsControlAssociations. Berikan ARN standar di mana Anda ingin menonaktifkan kontrol.
4. Atur `AssociationStatus` parameter sama dengan`DISABLED`. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah dinonaktifkan, API mengembalikan respons kode status HTTP 200.

   Contoh permintaan:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED",  "UpdatedReason": "Not applicable to environment"}]
}
```

AWS CLI

Untuk menonaktifkan kontrol dalam standar tertentu

1. Jalan list-security-control-definitions kan perintah, dan berikan ARN standar untuk mendapatkan daftar kontrol yang tersedia untuk standar tertentu. Untuk mendapatkan

ARN standar, jalankandescribe-standards. Perintah ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol khusus standar.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Jalan list-standards-control-associations kan perintah, dan berikan ID kontrol tertentu untuk mengembalikan status pengaktifan kontrol saat ini di setiap standar.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Jalankan perintah batch-update-standards-control-associations. Berikan ARN standar di mana Anda ingin menonaktifkan kontrol.
4. Atur AssociationStatus parameter sama denganDISABLED. Jika Anda mengikuti langkah-langkah ini untuk kontrol yang sudah diaktifkan, perintah mengembalikan respons kode status HTTP 200.

```
aws securityhub  --region us-east-1 batch-update-standards-control-
associations --standards-control-association-updates '[{"SecurityControlId":
 "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED",
 "UpdatedReason": "Not applicable to environment"}]'
```

Kontrol yang disarankan untuk dinonaktifkan di CSPM Security Hub

Sebaiknya nonaktifkan beberapa kontrol CSPM AWS Security Hub untuk mengurangi kebisingan dan biaya penggunaan.

Kontrol yang menggunakan sumber daya global

Beberapa Layanan AWS mendukung sumber daya global, yang berarti Anda dapat mengakses sumber daya dari mana punWilayah AWS. Untuk menghemat biayaAWS Config, Anda dapat menonaktifkan perekaman sumber daya global di semua kecuali satu Wilayah. Namun, setelah Anda melakukan ini, Security Hub CSPM masih menjalankan pemeriksaan keamanan di semua Wilayah di mana kontrol diaktifkan dan menagih Anda berdasarkan jumlah cek per akun per Wilayah. Dengan demikian, untuk mengurangi kebisingan dan menghemat biaya CSPM Security Hub, Anda juga harus

menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah yang mencatat sumber daya global.

Jika kontrol melibatkan sumber daya global tetapi hanya tersedia di satu Wilayah, menonaktifkannya di Wilayah tersebut mencegah Anda mendapatkan temuan apa pun untuk sumber daya yang mendasarinya. Dalam hal ini, kami sarankan untuk tetap mengaktifkan kontrol. Saat menggunakan agregasi lintas wilayah, Wilayah di mana kontrol tersedia harus merupakan Wilayah agregasi atau salah satu Wilayah yang ditautkan. Kontrol berikut melibatkan sumber daya global tetapi hanya tersedia di satu Wilayah:

- Semua CloudFront kontrol - Hanya tersedia di Wilayah AS Timur (Virginia N.)
- GlobalAccelerator.1— Hanya tersedia di Wilayah AS Barat (Oregon)
- Route53.2— Hanya tersedia di Wilayah AS Timur (Virginia N.)
- WAF.1, WAF.6, WAF.7, WAF.8 - Hanya tersedia di Wilayah AS Timur (Virginia N.)

> **Note**
>
> Jika Anda menggunakan konfigurasi pusat, Security Hub CSPM secara otomatis menonaktifkan kontrol yang melibatkan sumber daya global di semua Wilayah kecuali Wilayah asal. Kontrol lain yang Anda pilih untuk diaktifkan meskipun kebijakan konfigurasi diaktifkan di semua Wilayah yang tersedia. Untuk membatasi temuan untuk kontrol ini hanya pada satu Wilayah, Anda dapat memperbarui pengaturan AWS Config perekam dan menonaktifkan perekaman sumber daya global di semua Wilayah kecuali Wilayah asal.
> Jika kontrol yang diaktifkan yang melibatkan sumber daya global tidak didukung di Wilayah asal, CSPM Security Hub mencoba mengaktifkan kontrol di satu Wilayah tertaut di mana kontrol didukung. Dengan konfigurasi pusat, Anda tidak memiliki cakupan untuk kontrol yang tidak tersedia di Wilayah asal atau Wilayah yang ditautkan.
> Untuk informasi selengkapnya tentang konfigurasi pusat, lihatMemahami konfigurasi pusat di Security Hub CSPM.

Untuk kontrol yang memiliki jenis jadwal periodik, menonaktifkannya di Security Hub CSPM diperlukan untuk mencegah penagihan. Menyetel AWS Config parameter `includeGlobalResourceTypes` ke `false` tidak memengaruhi kontrol CSPM Security Hub berkala.

Kontrol CSPM Security Hub berikut menggunakan sumber daya global:

- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

CloudTrail kontrol logging

CloudTrail.2Kontrol mengevaluasi penggunaan AWS Key Management Service (AWS KMS) untuk mengenkripsi log AWS CloudTrail jejak. Jika Anda mencatat jejak ini di akun logging terpusat, Anda harus mengaktifkan kontrol ini hanya di akun dan di Wilayah AWS mana pencatatan terpusat terjadi.

Jika Anda menggunakan konfigurasi pusat, status pengaktifan kontrol disejajarkan di seluruh Wilayah beranda dan Wilayah yang ditautkan. Anda tidak dapat menonaktifkan kontrol di beberapa Wilayah dan mengaktifkannya di wilayah lain. Dalam hal ini, Anda dapat menekan temuan dari CloudTrail.2 kontrol untuk mengurangi kebisingan temuan.

CloudWatch kontrol alarm

Jika Anda lebih suka menggunakan Amazon GuardDuty untuk deteksi anomali daripada CloudWatch alarm Amazon, Anda dapat menonaktifkan kontrol berikut, yang berfokus pada alarm: CloudWatch

- [CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
- [CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah
- [CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA
- [CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM
- [CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi
- [CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi
- [CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan
- [CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
- [CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi
- [CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
- [CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
- [CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan
- [CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
- [CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC

Memahami pemeriksaan dan skor keamanan di Security Hub CSPM

Untuk setiap kontrol yang Anda aktifkan, AWS Security Hub CSPM menjalankan pemeriksaan keamanan. Pemeriksaan keamanan menghasilkan temuan yang memberi tahu Anda apakah AWS sumber daya tertentu sesuai dengan aturan yang termasuk dalam kontrol.

Beberapa pemeriksaan berjalan pada jadwal berkala. Pemeriksaan lain hanya berjalan ketika ada perubahan pada status sumber daya. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Banyak pemeriksaan keamanan menggunakan aturan AWS Config terkelola atau kustom untuk menetapkan persyaratan kepatuhan. Untuk menjalankan pemeriksaan ini, Anda harus mengatur AWS Config dan mengaktifkan perekaman sumber daya untuk sumber daya yang diperlukan. Untuk informasi lebih lanjut tentang pengaturanAWS Config, lihatMengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM. Untuk daftar AWS Config sumber daya yang harus Anda rekam untuk setiap standar, lihatDiperlukanAWS Configsumber daya untuk temuan kontrol. Kontrol lain menggunakan fungsi Lambda khusus, yang dikelola oleh Security Hub CSPM dan tidak memerlukan prasyarat apa pun.

Karena Security Hub CSPM menjalankan pemeriksaan keamanan, CSPM menghasilkan temuan dan memberi mereka status kepatuhan. Untuk informasi selengkapnya tentang status kepatuhan, lihatMengevaluasi status kepatuhan temuan CSPM Security Hub.

Security Hub CSPM menggunakan status kepatuhan temuan kontrol untuk menentukan status kontrol secara keseluruhan. Berdasarkan status kontrol, Security Hub CSPM juga menghitung skor keamanan di semua kontrol yang diaktifkan dan untuk standar tertentu. Untuk informasi selengkapnya, lihat the section called “Status kepatuhan dan status kontrol” dan the section called “Menghitung skor keamanan”.

Jika Anda mengaktifkan temuan kontrol konsolidasi, Security Hub CSPM menghasilkan satu temuan bahkan ketika kontrol dikaitkan dengan lebih dari satu standar. Lihat informasi yang lebih lengkap di Temuan kontrol konsolidasi.

Topik

- DiperlukanAWS Configsumber daya untuk temuan kontrol
- Jadwal untuk menjalankan pemeriksaan keamanan
- Menghasilkan dan memperbarui temuan kontrol
- Mengevaluasi status kepatuhan dan status kontrol
- Menghitung skor keamanan

DiperlukanAWS Configsumber daya untuk temuan kontrol

> **Note**
>
> Jika Anda menggunakan Security Hub CSPM dan Security Hub konfigurasi rekaman sumber daya dikelola untuk Anda. Security Hub membuat perekam konfigurasi terkait layanan dengan AWS Config dan mendapatkan informasi langsung tentang semua sumber daya yang terkait dengan kontrol yang didukung di Security Hub CSPM. Untuk informasi selengkapnya, lihat Menggunakan perekam konfigurasi terkait layanan.

Di CSPM AWS Security Hub, beberapa kontrol menggunakan AWS Config aturan terkait layanan yang mendeteksi perubahan konfigurasi dalam sumber daya Anda. AWS Agar CSPM Security Hub menghasilkan temuan akurat untuk kontrol ini, Anda harus mengaktifkan AWS Config dan mengaktifkan perekaman sumber daya. AWS Config Untuk informasi tentang cara Security Hub CSPM menggunakan AWS Config aturan dan cara mengaktifkan dan mengonfigurasiAWS Config, lihat. Mengaktifkan dan mengkonfigurasi AWS Config untuk Security Hub CSPM Untuk informasi rinci tentang perekaman sumber daya, lihat Bekerja dengan perekam konfigurasi di Panduan AWS Config Pengembang.

Untuk menerima temuan kontrol yang akurat, Anda harus mengaktifkan perekaman AWS Config sumber daya untuk kontrol yang diaktifkan dengan jenis jadwal yang dipicu perubahan. Beberapa kontrol dengan jenis jadwal periodik juga memerlukan perekaman sumber daya. Halaman ini mencantumkan sumber daya yang diperlukan untuk kontrol CSPM Security Hub ini.

Kontrol CSPM Security Hub dapat mengandalkan AWS Config aturan terkelola atau aturan CSPM Security Hub kustom. Pastikan tidak ada kebijakan AWS Identity and Access Management (IAM) atau kebijakan AWS Organizations terkelola yang AWS Config mencegah izin untuk merekam sumber daya Anda. Kontrol CSPM Security Hub mengevaluasi konfigurasi sumber daya secara langsung dan tidak memperhitungkan AWS Organizations kebijakan.

> **Note**
>
> Di Wilayah AWS mana kontrol tidak tersedia, sumber daya yang sesuai tidak tersedia diAWS Config. Untuk daftar batasan ini, lihatBatasan regional pada kontrol CSPM Security Hub.

Topik

- Sumber daya yang diperlukan untuk semua kontrol CSPM Security Hub
- Sumber daya yang dibutuhkan untukAWSStandar Praktik Terbaik Keamanan Dasar
- Sumber daya yang dibutuhkan untuk CISAWSTolok Ukur Yayasan
- Sumber daya yang diperlukan untuk standar NIST SP 800-53 Revisi 5
- Sumber daya yang diperlukan untuk standar NIST SP 800-171 Revisi 2
- Sumber daya yang dibutuhkan untuk PCI DSS v3.2.1
- Sumber daya yang dibutuhkan untukAWSStandar Penandaan Sumber Daya

Sumber daya yang diperlukan untuk semua kontrol CSPM Security Hub

Agar CSPM Security Hub menghasilkan temuan untuk kontrol yang dipicu perubahan yang diaktifkan dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config Tabel ini juga menunjukkan kontrol mana yang mengevaluasi jenis sumber daya tertentu. Kontrol tunggal dapat mengevaluasi lebih dari satu jenis sumber daya.

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Amplify	`AWS::Amplify::App`	Amplify.1
	`AWS::Amplify::Branch`	Amplify.2
Amazon API Gateway	`AWS::ApiGateway::Stage`	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	`AWS::ApiGatewayV2::Stage`	APIGateway.1 APIGateway.9

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::ApiGateway::DomainName`	APIGateway.11
AWS AppConfig	`AWS::AppConfig::Application`	AppConfig.1
	`AWS::AppConfig::ConfigurationProfile`	AppConfig.2
	`AWS::AppConfig::Environment`	AppConfig.3
	`AWS::AppConfig::ExtensionAssociation`	AppConfig.4
Amazon AppFlow	`AWS::AppFlow::Flow`	AppFlow.1
AWS App Runner	`AWS::AppRunner::Service`	AppRunner.1
	`AWS::AppRunner::VpcConnector`	AppRunner.2
AWS AppSync	`AWS::AppSync::GraphQLApi`	AppSync.2 AppSync.4 AppSync.5

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::AppSync::ApiCache`	AppSync.1 AppSync.6
AWS Backup	`AWS::Backup::BackupPlan`	Backup.5
	`AWS::Backup::BackupVault`	Backup.3
	`AWS::Backup::RecoveryPoint`	Backup.1 Backup.2
	`AWS::Backup::ReportPlan`	Backup.4
AWS Batch	`AWS::Batch::ComputeEnvironment`	Batch.3 Batch.4
	`AWS::Batch::JobQueue`	Batch.1
	`AWS::Batch::SchedulingPolicy`	Batch.2
Amazon Bedrock	`AWS::Bedrock::DataSource`	Bedrock.1
Batuan Dasar Amazon AgentCore	`AWS::BedrockAgentCore::BrowserCustom`	BedrockAgentCore.5 BedrockAgentCore.6

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::BedrockAgentCore::CodeInterpreterCustom`	BedrockAgentCore.7
	`AWS::BedrockAgentCore::Gateway`	BedrockAgentCore.2 BedrockAgentCore.4
	`AWS::BedrockAgentCore::Memory`	BedrockAgentCore.3
	`AWS::BedrockAgentCore::Runtime`	BedrockAgentCore.1
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`	ACM.1 ACM.2 ACM.3
Amazon Athena	`AWS::Athena::DataCatalog`	Athena.2
	`AWS::Athena::WorkGroup`	Athena.3 Athena.4
AWS CloudFormation	`AWS::CloudFormation::Stack`	CloudFormation.2 CloudFormation.3 CloudFormation.4

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon CloudFront	`AWS::CloudFront::Distribution`	CloudFront.1 CloudFront.3 CloudFront.4 CloudFront.5 CloudFront.6 CloudFront.7 CloudFront.8 CloudFront.9 CloudFront.10 CloudFront.13 CloudFront.14 CloudFront.15 CloudFront.16 CloudFront.17
AWS CloudTrail	`AWS::CloudTrail::Trail`	CloudTrail.9
	`AWS::CloudTrail::EventDataStore`	CloudTrail.11
Amazon CloudWatch	`AWS::CloudWatch::Alarm`	CloudWatch.15 CloudWatch.17

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS CodeArtifact	`AWS::CodeArtifact::Repository`	CodeArtifact.1
AWS CodeBuild	`AWS::CodeBuild::Project`	CodeBuild.1 CodeBuild.2 CodeBuild.3 CodeBuild.4
	`AWS::CodeBuild::ReportGroup`	CodeBuild.7
Amazon CodeGuru Profiler	`AWS::CodeGuruProfiler::ProfilingGroup`	CodeGuruProfiler.1
CodeGuru Peninjau Amazon	`AWS::CodeGuruReviewer::RepositoryAssociation`	CodeGuruReviewer.1
Amazon Cognito	`AWS::Cognito::IdentityPool`	Cognito.2

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::Cognito::UserPool`	Cognito.1 Cognito.3 Cognito.4 Cognito.5 Cognito.6
Pelanggan Amazon Connect	`AWS::CustomerProfiles::ObjectType`	Connect.1
	`AWS::Connect::Instance`	Connect.2
AWS DataSync	`AWS::DataSync::Task`	DataSync.1 DataSync.2
Amazon Detective	`AWS::Detective::Graph`	Detective.1
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Certificate`	DMS.2
	`AWS::DMS::Endpoint`	DMS.9 DMS.10 DMS.11 DMS.12
	`AWS::DMS::EventSubscription`	DMS.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::DMS::ReplicationInstance`	DMS.4 DMS.6 DMS.13
	`AWS::DMS::ReplicationSubnetGroup`	DMS.5
	`AWS::DMS::ReplicationTask`	DMS.7 DMS.8
Amazon DynamoDB	`AWS::DynamoDB::Table`	DynamoDB.1 DynamoDB.2 DynamoDB.5 DynamoDB.6
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::ClientVpnEndpoint`	EC2.51
	`AWS::EC2::CustomerGateway`	EC2.36
	`AWS::EC2::DHCPOptions`	EC2.174
	`AWS::EC2::EIP`	EC2.12 EC2.37

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::EC2::FlowLog`	EC2.48
	`AWS::EC2::Instance`	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2.38 EMR.1 SSM.1
	`AWS::EC2::InternetGateway`	EC2.39
	`AWS::EC2::LaunchTemplate`	EC2.25 EC2.170 EC2.175 EC2.181
	`AWS::EC2::NatGateway`	EC2.40
	`AWS::EC2::NetworkAcl`	EC2.16 EC2.21 EC2.41

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::EC2::NetworkInterface	EC2.22 EC2.35 EC2.180
	AWS::EC2::PrefixList	EC2.176
	AWS::EC2::RouteTable	EC2.42
	AWS::EC2::SecurityGroup	EC2.2 EC2.13 EC2.14 EC2.18 EC2.19 EC2.43
	AWS::EC2::SnapshotBlockPublicAccess	EC2.182
	AWS::EC2::SpotFleet	EC2.173
	AWS::EC2::Subnet	EC2.15 EC2.44 ElastiCache.7

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::EC2::TrafficMirrorFilter	EC2.178
	AWS::EC2::TrafficMirrorSession	EC2.177
	AWS::EC2::TrafficMirrorTarget	EC2.179
	AWS::EC2::TransitGateway	EC2.23 EC2.52
	AWS::EC2::TransitGatewayAttachment	EC2.33
	AWS::EC2::TransitGatewayRouteTable	EC2.34
	AWS::EC2::Volume	EC2.3 EC2.45
	AWS::EC2::VPC	EC2.6 EC2.46

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::EC2::VPCBlockPublicAccessOptions`	EC2.172
	`AWS::EC2::VPCEndpointService`	EC2.47
	`AWS::EC2::VPCPeeringConnection`	EC2.49
	`AWS::EC2::VPNConnection`	EC2.20 EC2.171 EC2.183
	`AWS::EC2::VPNGateway`	EC2.50
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`	AutoScaling.1 AutoScaling.2 AutoScaling.6 AutoScaling.9 AutoScaling.10
	`AWS::AutoScaling::LaunchConfiguration`	AutoScaling.3 Autoscaling.5

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance`	SSM.3
	`AWS::SSM::ManagedInstanceInventory`	SSM.1
	`AWS::SSM::PatchCompliance`	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`	ECR.4
	`AWS::ECR::Repository`	ECR.2 ECR.3 ECR.5
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster`	ECS.12 ECS.14
	`AWS::ECS::CapacityProvider`	ECS.19
	`AWS::ECS::Service`	ECS.2 ECS.10 ECS.13

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::ECS::TaskDefinition`	ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15 ECS.17 ECS.18 ECS.20 ECS.21
	`AWS::ECS::TaskSet`	ECS.16
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`	EFS.3 EFS.4 EFS.5
	`AWS::EFS::FileSystem`	EFS.7 EFS.8
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`	EKS.2 EKS.6 EKS.8

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::EKS::Identity ProviderConfig`	EKS.7
	`AWS::EKS::Nodegroup`	EKS.9
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`	ElasticBeanstalk.1 ElasticBeanstalk.2 ElasticBeanstalk.3
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	`AWS::ElasticLoadBalancingV2::Listener`	ELB.17 ELB.18

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::ElasticLoadBalancingV2::LoadBalancer`	ELB.1 ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 ELB.16
ElasticSearch	`AWS::Elasticsearch::Domain`	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EMR	`AWS::EMR::SecurityConfiguration`	EMR.3 EMR.4
Amazon EventBridge	`AWS::Events::EventBus`	EventBridge.2 EventBridge.3
	`AWS::Events::Endpoint`	EventBridge.4

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Fraud Detector	`AWS::FraudDetector::EntityType`	FraudDetector.1
	`AWS::FraudDetector::Label`	FraudDetector.2
	`AWS::FraudDetector::Outcome`	FraudDetector.3
	`AWS::FraudDetector::Variable`	FraudDetector.4
AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`	GlobalAccelerator.1
AWS Glue	`AWS::Glue::Job`	Glue.1 Glue.4
	`AWS::Glue::MLTransform`	Glue.3
Amazon GuardDuty	`AWS::GuardDuty::Detector`	GuardDuty.4
	`AWS::GuardDuty::Filter`	GuardDuty.2
	`AWS::GuardDuty::IPSet`	GuardDuty.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Identity and Access Managemen t(IAM)	`AWS::IAM::Group`	IAM.27 KMS.2
	`AWS::IAM: :Policy`	IAM.1 IAM.21 KMS.1
	`AWS::IAM::Role`	IAM.24 IAM.27 KMS.2
	`AWS::IAM::User`	IAM.2 IAM.3 IAM.5 IAM.8 IAM.19 IAM.22 IAM.25 IAM.27 KMS.2
AWS Identity and Access Management Access Analyzer	`AWS::Acce ssAnalyze r::Analyzer`	IAM.23

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::PlaybackKeyPair`	IVS.1
	`AWS::IVS::RecordingConfiguration`	IVS.2
	`AWS::IVS::Channel`	IVS.3
AWS IoT	`AWS::IoT::Authorizer`	IoT.4
	`AWS::IoT::Dimension`	IoT.3
	`AWS::IoT::MitigationAction`	IoT.2
	`AWS::IoT::Policy`	IoT.6
	`AWS::IoT::RoleAlias`	IoT.5
	`AWS::IoT::SecurityProfile`	IoT.1
AWSIoT Events	`AWS::IoTEvents::AlarmModel`	IoTEvents.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::IoTEvents::DetectorModel`	IoTEvents.2
	`AWS::IoTEvents::Input`	IoTEvents.1
AWSIoT SiteWise	`AWS::IoTSiteWise::AssetModel`	IoTSiteWise.1
	`AWS::IoTSiteWise::Dashboard`	IoTSiteWise.2
	`AWS::IoTSiteWise::Gateway`	IoTSiteWise.3
	`AWS::IoTSiteWise::Portal`	IoTSiteWise.4
	`AWS::IoTSiteWise::Project`	IoTSiteWise.5
AWSIoT TwinMaker	`AWS::IoTTwinMaker::Entity`	IoTTwinMaker.4
	`AWS::IoTTwinMaker::Scene`	IoTTwinMaker.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::IoTTwinMaker::SyncJob`	IoTTwinMaker.1
	`AWS::IoTTwinMaker::Workspace`	IoTTwinMaker.2
AWSIoT Wireless	`AWS::IoTWireless::MulticastGroup`	IoTWireless.1
	`AWS::IoTWireless::ServiceProfile`	IoTWireless.2
	`AWS::IoTWireless::FuotaTask`	IoTWireless.3
Amazon Keyspaces (untuk Apache Cassandra)	`AWS::Cassandra::Keyspace`	Keyspaces.1
Amazon Kinesis	`AWS::Kinesis::Stream`	Kinesis.1 Kinesis.2 Kinesis.3
AWS Key Management Service(AWS KMS)	`AWS::KMS::Alias`	S3.17
	`AWS::KMS::Key`	KMS.3 KMS.5 S3.17

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Lambda	`AWS::Lambda::Function`	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6 Lambda.7
Amazon MSK	`AWS::MSK::Cluster`	MSK.1 MSK.2 MSK.4 MSK.6
	`AWS::KafkaConnect::Connector`	MSK.3 MSK.5
Amazon MQ	`AWS::AmazonMQ::Broker`	MQ.2 MQ.4 MQ.5 MQ.6
AWS Network Firewall	`AWS::NetworkFirewall::Firewall`	NetworkFirewall.1 NetworkFirewall.7 NetworkFirewall.9 NetworkFirewall.10

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::NetworkFirewall::FirewallPolicy`	NetworkFirewall.3 NetworkFirewall.4 NetworkFirewall.5 NetworkFirewall.8
	`AWS::NetworkFirewall::RuleGroup`	NetworkFirewall.6
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Opensearch.9 Opensearch.10 Opensearch.11
AWS Private CA	`AWS::ACMPCA::CertificateAuthority`	PCA.2

Layanan AWS	Jenis sumber daya	Kontrol terkait
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster`	DocumentDB.1 DocumentDB.2 DocumentDB.4 DocumentDB.5 Neptune.1 Neptune.2 Neptune.4 Neptune.5 Neptune.7 Neptune.8 Neptune.9 RDS.7 RDS.12 RDS.14 RDS.15 RDS.16 RDS.24 RDS.27 RDS.28 RDS.34 RDS.35

Layanan AWS	Jenis sumber daya	Kontrol terkait
		RDS.37 RDS.47 RDS.48
	`AWS::RDS::DBClusterSnapshot`	DocumentDB.3 Neptune.3 Neptune.6 RDS.1 RDS.4 RDS.29

Layanan AWS	Jenis sumber daya	Kontrol terkait
	AWS::RDS::DBInstance	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.23 RDS.25 RDS.30 RDS.36 RDS.40
	AWS::RDS::DBSecurityGroup	RDS.31
	AWS::RDS::DBSnapshot	RDS.1 RDS.4 RDS.32

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::RDS::DBSubnetGroup`	RDS.33
	`AWS::RDS::EventSubscription`	RDS.19 RDS.20 RDS.21 RDS.22
	`AWS::RDS::GlobalCluster`	RDS.51
Amazon Redshift	`AWS::Redshift::Cluster`	Redshift.1 Redshift.2 Redshift.3 Redshift.4 Redshift.6 Redshift.7 Redshift.8 Redshift.10 Redshift.11 Redshift.18
	`AWS::Redshift::ClusterParameterGroup`	Redshift.2 Redshift.17

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::Redshift::ClusterSnapshot`	Redshift.13
	`AWS::Redshift::ClusterSubnetGroup`	Redshift.14 Redshift.16
	`AWS::Redshift::EventSubscription`	Redshift.12
Amazon Route 53	`AWS::Route53::HostedZone`	Route53.2
	`AWS::Route53::HealthCheck`	Route53.1
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint`	S3.19
	`AWS::S3::AccountPublicAccessBlock`	S3.2 S3.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::S3::Bucket`	CloudTrail.6 CloudTrail.7 S3.2 S3.3 S3.5 S3.6 S3.7 S3.8 S3.9 S3.10 S3.11 S3.12 S3.13 S3.14 S3.15 S3.17 S3.20
	`AWS::S3::MultiRegionAccessPoint`	S3.24

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::S3Express::DirectoryBucket`	S3.25
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig`	SageMaker.6
	`AWS::SageMaker::Image`	SageMaker.7
	`AWS::SageMaker::InferenceExperiment`	SageMaker.23 SageMaker.24
	`AWS::SageMaker::Model`	SageMaker.5 SageMaker.16 SageMaker.19
	`AWS::SageMaker::ModelExplainabilityJobDefinition`	SageMaker.20
	`AWS::SageMaker::ModelQualityJobDefinition`	SageMaker.25
	`AWS::SageMaker::MonitoringSchedule`	SageMaker.22

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::SageMaker::NotebookInstance`	SageMaker.2 SageMaker.3 SageMaker.21
	`AWS::SageMaker::FeatureGroup`	SageMaker.17 SageMaker.18
AWS Secrets Manager	`AWS::SecretsManager::Secret`	SecretsManager.1 SecretsManager.2 SecretsManager.5
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`	ServiceCatalog.1
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet`	SES.2 SES.3
	`AWS::SES::ContactList`	SES.1
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`	SNS.1 SNS.3 SNS.4
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`	SQS.1 SQS.2 SQS.3

Layanan AWS	Jenis sumber daya	Kontrol terkait
AWS Step Functions	`AWS::StepFunctions::StateMachine`	StepFunctions.1
	`AWS::StepFunctions::Activity`	StepFunctions.2
AWS Systems Manager(SSM)	`AWS::SSM::Document`	SSM.5
AWS Transfer Family	`AWS::Transfer::Agreement`	Transfer.4
	`AWS::Transfer::Certificate`	Transfer.5
	`AWS::Transfer::Connector`	Transfer.3 Transfer.6
	`AWS::Transfer::Profile`	Transfer.7
	`AWS::Transfer::Workflow`	Transfer.1
AWS WAF	`AWS::WAF::Rule`	WAF.6
	`AWS::WAF::RuleGroup`	WAF.7
	`AWS::WAF::WebACL`	WAF.1 WAF.8

Layanan AWS	Jenis sumber daya	Kontrol terkait
	`AWS::WAFRegional::Rule`	WAF.2
	`AWS::WAFRegional::RuleGroup`	WAF.3
	`AWS::WAFRegional::WebACL`	WAF.4
	`AWS::WAFv2::RuleGroup`	WAF.12
	`AWS::WAFv2::WebACL`	WAF.10 WAF.11
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`	WorkSpaces.1 WorkSpaces.2

Sumber daya yang dibutuhkan untukAWSStandar Praktik Terbaik Keamanan Dasar

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan yang berlaku pada standar Praktik Terbaik Keamanan AWS Dasar (v.1.0.0), diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut ini. AWS Config Untuk informasi tentang standar ini, lihatAWS Standar Praktik Terbaik Keamanan Dasar di Security Hub CSPM.

Layanan AWS	Jenis sumber daya
Amazon API Gateway	`AWS::ApiGateway::DomainName` , `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`

Layanan AWS	Jenis sumber daya
AWS AppSync	`AWS::AppSync::ApiCache` , `AWS::AppSync::GraphQLApi`
AWS Backup	`AWS::Backup::RecoveryPoint`
Amazon Bedrock	`AWS::Bedrock::DataSource`
Batuan Dasar Amazon AgentCore	`AWS::BedrockAgentCore::BrowserCustom` , `AWS::BedrockAgentCore::CodeInterpreterCustom` , `AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Runtime`
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CodeBuild	`AWS::CodeBuild::Project` , `AWS::CodeBuild::ReportGroup`
Amazon Cognito	`AWS::Cognito::IdentityPool` , `AWS::Cognito::UserPool`
AWS CloudTrail	`AWS::CloudTrail::EventDataStore`
Pelanggan Amazon Connect	`AWS::Connect::Instance`
AWS DataSync	`AWS::DataSync::Task`
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`

Layanan AWS	Jenis sumber daya
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::SnapshotBlockPublicAccess` , `AWS::EC2::SpotFleet` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPCBlockPublicAccessOptions` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::CapacityProvider` , `AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition` , `AWS::ECS::TaskSet`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint` , `AWS::EFS::FileSystem`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::Nodegroup`

Layanan AWS	Jenis sumber daya
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
AWS Glue	`AWS::Glue::Job` , `AWS::Glue::MLTransform`
AWS Identity and Access Management(IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Key Management Service(AWS KMS)	`AWS::KMS::Key`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster` , `AWS::KafkaConnect::Connector`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`

Layanan AWS	Jenis sumber daya
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBProxy` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription` , `AWS::RDS::GlobalCluster`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Redshift Tanpa Server	`AWS::RedshiftServerless::Workgroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket` , `AWS::S3::MultiRegionAccessPoint` , `AWS::S3Express::DirectoryBucket`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::InferenceExperiment` , `AWS::SageMaker::Model` , `AWS::SageMaker::ModelExplainabilityJobDefinition` , `AWS::SageMaker::ModelQualityJobDefinition` , `AWS::SageMaker::MonitoringSchedule` , `AWS::SageMaker::NotebookInstance`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`

Layanan AWS	Jenis sumber daya
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Step Functions	`AWS::StepFunctions::StateMachine`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`
Amazon WorkSpaces	`AWS::WorkSpaces::WorkSpace`

Sumber daya yang dibutuhkan untuk CISAWSTolok Ukur Yayasan

Untuk menjalankan pemeriksaan keamanan untuk kontrol yang diaktifkan yang berlaku untuk Tolok Ukur AWS Yayasan Center for Internet Security (CIS), Security Hub CSPM berjalan melalui langkah-langkah audit yang tepat yang ditentukan untuk pemeriksaan atau menggunakan aturan terkelola tertentu. AWS Config Untuk informasi tentang standar ini di Security Hub CSPM, lihat. CIS AWS Benchmark Yayasan di Hub Keamanan CSPM

Sumber daya yang diperlukan untuk CIS v5.0.0

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v5.0.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut ini. AWS Config

Layanan AWS	Jenis sumber daya
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::FileSystem`

Layanan AWS	Jenis sumber daya
AWS Identity and Access Management(IAM)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance` , `AWS::RDS::DBCluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Sumber daya yang dibutuhkan untuk CIS v3.0.0

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v3.0.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut ini. AWS Config

Layanan AWS	Jenis sumber daya
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::Instance` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC`
AWS Identity and Access Management(IAM)	`AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Sumber daya yang dibutuhkan untuk CIS v1.4.0

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v1.4.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut ini. AWS Config

Layanan AWS	Jenis sumber daya
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBInstance`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::Bucket`

Sumber daya yang diperlukan untuk CIS v1.2.0

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan CIS v1.2.0 yang diaktifkan yang menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut ini. AWS Config

Layanan AWS	Jenis sumber daya
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::SecurityGroup`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

Sumber daya yang diperlukan untuk standar NIST SP 800-53 Revisi 5

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan yang berlaku pada standar NIST SP 800-53 Revisi 5, diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config Untuk informasi tentang standar ini, lihatNIST SP 800-53 Revisi 5 di Hub Keamanan CSPM.

Layanan AWS	Jenis sumber daya
Amazon API Gateway	`AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage`
AWS AppSync	`AWS::AppSync::GraphQLApi`

Layanan AWS	Jenis sumber daya
AWS Backup	`AWS::Backup::RecoveryPoint`
Batuan Dasar Amazon AgentCore	`AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Memory`
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
AWS CodeBuild	`AWS::CodeBuild::Project`
AWS Database Migration Service(AWS DMS)	`AWS::DMS::Endpoint` , `AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationTask`
Amazon DynamoDB	`AWS::DynamoDB::Table`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::Repository`

Layanan AWS	Jenis sumber daya
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer` , `AWS::ElasticLoadBalancingV2::Listener` , `AWS::ElasticLoadBalancingV2::LoadBalancer`
Amazon ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EMR	`AWS::EMR::SecurityConfiguration`
Amazon EventBridge	`AWS::Events::Endpoint` , `AWS::Events::EventBus`
AWS Glue	`AWS::Glue::Job`
AWS Identity and Access Management(IAM)	`AWS::IAM::Group` , `AWS::IAM::Policy` , `AWS::IAM::Role` , `AWS::IAM::User`
AWS Key Management Service(AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`
Amazon Managed Streaming for Apache Kafka (Amazon MSK)	`AWS::MSK::Cluster`

Layanan AWS	Jenis sumber daya
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot` , `AWS::RDS::EventSubscription`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterSubnetGroup`
Amazon Route 53	`AWS::Route53::HostedZone`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccessPoint` , `AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
AWS Service Catalog	`AWS::ServiceCatalog::Portfolio`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`
Amazon SageMaker AI	`AWS::SageMaker::FeatureGroup` , `AWS::SageMaker::NotebookInstance`

Layanan AWS	Jenis sumber daya
AWS Secrets Manager	`AWS::SecretsManager::Secret`
AWS Transfer Family	`AWS::Transfer::Connector`
AWS WAF	`AWS::WAF::Rule` , `AWS::WAF::RuleGroup` , `AWS::WAF::WebACL` , `AWS::WAFRegional::Rule` , `AWS::WAFRegional::RuleGroup` , `AWS::WAFRegional::WebACL` , `AWS::WAFv2::RuleGroup` , `AWS::WAFv2::WebACL`

Sumber daya yang diperlukan untuk standar NIST SP 800-171 Revisi 2

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang dipicu perubahan yang berlaku pada standar NIST SP 800-171 Revisi 2, diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut. AWS Config Untuk informasi tentang standar ini, lihatNIST SP 800-171 Revisi 2 di Hub Keamanan CSPM.

Layanan AWS	Jenis sumber daya
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
Amazon API Gateway	`AWS::ApiGateway::Stage`
Amazon CloudFront	`AWS::CloudFront::Distribution`
Amazon CloudWatch	`AWS::CloudWatch::Alarm`
Awan Komputasi Elastis Amazon (Amazon EC2)	`AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection`
Elastic Load Balancing	`AWS::ElasticLoadBalancing::LoadBalancer`

Layanan AWS	Jenis sumber daya
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`
AWS Key Management Service (AWS KMS)	`AWS::KMS::Alias` , `AWS::KMS::Key`
AWS Network Firewall	`AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup`
Layanan Penyimpanan Sederhana Amazon (Amazon S3)	`AWS::S3::Bucket`
Layanan Pemberitahuan Sederhana Amazon (Amazon SNS)	`AWS::SNS::Topic`
AWS Systems Manager(SSM)	`AWS::SSM::PatchCompliance`
AWS WAF	`AWS::WAFv2::RuleGroup`

Sumber daya yang dibutuhkan untuk PCI DSS v3.2.1

Agar CSPM Security Hub melaporkan temuan secara akurat untuk kontrol yang berlaku untuk v3.2.1 Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), diaktifkan, dan menggunakan AWS Config aturan, Anda harus mencatat jenis sumber daya berikut di. AWS Config Untuk informasi tentang standar ini, lihatPCI DSS di Hub Keamanan CSPM.

Layanan AWS	Jenis sumber daya
AWS CodeBuild	`AWS::CodeBuild::Project`
Amazon Elastic Compute Cloud (Amazon EC2)	`AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::SecurityGroup`
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
AWS Identity and Access Management(IAM)	`AWS::IAM::Policy` , `AWS::IAM::User`

Layanan AWS	Jenis sumber daya
AWS Lambda	`AWS::Lambda::Function`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`
Amazon Relational Database Service (Amazon RDS)	`AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSnapshot`
Amazon Redshift	`AWS::Redshift::Cluster`
Amazon Simple Storage Service (Amazon S3)	`AWS::S3::AccountPublicAccessBlock` , `AWS::S3::Bucket`
Amazon EC2 Systems Manager (SSM)	`AWS::SSM::AssociationCompliance` , `AWS::SSM::ManagedInstanceInventory` , `AWS::SSM::PatchCompliance`

Sumber daya yang dibutuhkan untukAWSStandar Penandaan Sumber Daya

Semua kontrol yang berlaku untuk standar AWS Resource Tagging dipicu perubahan dan menggunakan AWS Config aturan. Agar CSPM Security Hub melaporkan temuan untuk kontrol ini secara akurat, Anda harus mencatat jenis sumber daya berikut. AWS Config Untuk informasi tentang standar ini, lihatAWS Standar Penandaan Sumber Daya di Security Hub CSPM.

Layanan AWS	Jenis sumber daya
AWS Amplify	`AWS::Amplify::App` , `AWS::Amplify::Branch`
Amazon AppFlow	`AWS::AppFlow::Flow`
AWS App Runner	`AWS::AppRunner::Service` , `AWS::AppRunner::VpcConnector`
AWS AppConfig	`AWS::AppConfig::Application` , `AWS::AppConfig::Configurati`

Layanan AWS	Jenis sumber daya
	`onProfile` , `AWS::AppConfig::Environment` , `AWS::AppConfig::ExtensionAssociation`
AWS AppSync	`AWS::AppSync::GraphQLApi`
Amazon Athena	`AWS::Athena::DataCatalog` , `AWS::Athena::WorkGroup`
AWS Backup	`AWS::Backup::BackupPlan` , `AWS::Backup::BackupVault` , `AWS::Backup::RecoveryPlan` , `AWS::Backup::ReportPlan`
AWS Batch	`AWS::Batch::ComputeEnvironment` , `AWS::Batch::JobQueue` , `AWS::Batch::SchedulingPolicy`
AWS Certificate Manager(ACM)	`AWS::ACM::Certificate`
AWS CloudFormation	`AWS::CloudFormation::Stack`
Amazon CloudFront	`AWS::CloudFront::Distribution`
AWS CloudTrail	`AWS::CloudTrail::Trail`
AWS CodeArtifact	`AWS::CodeArtifact::Repository`
Amazon CodeGuru	`AWS::CodeGuruProfiler::ProfilingGroup` , `AWS::CodeGuruReviewer::RepositoryAssociation`
Pelanggan Amazon Connect	`AWS::CustomerProfiles::ObjectType`

Layanan AWS	Jenis sumber daya

AWS Database Migration Service(AWS DMS)	`AWS::DMS::Certificate` , `AWS::DMS::EventSubscription`
	
	`AWS::DMS::ReplicationInstance` , `AWS::DMS::ReplicationSubnetGroup`

AWS DataSync	`AWS::DataSync::Task`
Amazon Detective	`AWS::Detective::Graph`
Amazon DynamoDB	`AWS::DynamoDB::Trail`
Amazon Elastic Compute Cloud (EC2)	`AWS::EC2::CustomerGateway` , `AWS::EC2::DHCPOptions` , `AWS::EC2::EIP` , `AWS::EC2::FlowLog` , `AWS::EC2::Instance` , `AWS::EC2::InternetGateway` , `AWS::EC2::LaunchTemplate` , `AWS::EC2::NatGateway` , `AWS::EC2::NetworkAcl` , `AWS::EC2::NetworkInterface` , `AWS::EC2::PrefixList` , `AWS::EC2::RouteTable` , `AWS::EC2::SecurityGroup` , `AWS::EC2::Subnet` , `AWS::EC2::TrafficMirrorFilter` , `AWS::EC2::TrafficMirrorSession` , `AWS::EC2::TrafficMirrorTarget` , `AWS::EC2::TransitGateway` , `AWS::EC2::TransitGatewayAttachment` , `AWS::EC2::TransitGatewayRouteTable` , `AWS::EC2::Volume` , `AWS::EC2::VPC` , `AWS::EC2::VPCEndpointService` , `AWS::EC2::VPCPeeringConnection` , `AWS::EC2::VPNGateway`

Layanan AWS	Jenis sumber daya
Amazon EC2 Auto Scaling	`AWS::AutoScaling::AutoScalingGroup`
Amazon Elastic Container Registry (Amazon ECR)	`AWS::ECR::PublicRepository`
Amazon Elastic Container Service (Amazon ECS)	`AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition`
Amazon Elastic File System (Amazon EFS)	`AWS::EFS::AccessPoint`
Amazon Elastic Kubernetes Service (Amazon EKS)	`AWS::EKS::Cluster` , `AWS::EKS::IdentityProviderConfig`
AWS Elastic Beanstalk	`AWS::ElasticBeanstalk::Environment`
ElasticSearch	`AWS::Elasticsearch::Domain`
Amazon EventBridge	`AWS::Events::EventBus`

Amazon Fraud Detector	`AWS::FraudDetector::EntityType` , `AWS::FraudDetector::Label`
	
	`AWS::FraudDetector::Outcome` , `AWS::FraudDetector::Variable`

AWS Global Accelerator	`AWS::GlobalAccelerator::Accelerator`
AWS Glue	`AWS::Glue::Job`
Amazon GuardDuty	`AWS::GuardDuty::Detector` , `AWS::GuardDuty::Filter` , `AWS::GuardDuty::IPSet`
AWS Identity and Access Management(IAM)	`AWS::IAM::Role` , `AWS::IAM::User`

Layanan AWS	Jenis sumber daya
AWS Identity and Access Management Access Analyzer(Penganalisis Akses IAM)	`AWS::AccessAnalyzer::Analyzer`
AWS IoT	`AWS::IoT::Authorizer` , `AWS::IoT::Dimension` , `AWS::IoT::MitigationAction` , `AWS::IoT::Policy` , `AWS::IoT::RoleAlias` , `AWS::IoT::SecurityProfile`
AWS IoTAcara	`AWS::IoTEvents::AlarmModel` , `AWS::IoTEvents::DetectorModel` , `AWS::IoTEvents::Input`
AWS IoTSiteWise	`AWS::IoTSiteWise::Dashboard` , `AWS::IoTSiteWise::Gateway` , `AWS::IoTSiteWise::Portal` , `AWS::IoTSiteWise::Project`
AWS IoTTwinMaker	`AWS::IoTTwinMaker::Entity` , `AWS::IoTTwinMaker::Scene` , `AWS::IoTTwinMaker::SyncJob` , `AWS::IoTTwinMaker::Workspace`
AWS IoTNirkabel	`AWS::IoTWireless::FuotaTask` , `AWS::IoTWireless::MulticastGroup` , `AWS::IoTWireless::ServiceProfile`
Amazon Interactive Video Service (Amazon IVS)	`AWS::IVS::Channel` , `AWS::IVS::PlaybackKeyPair` , `AWS::IVS::RecordingConfiguration`
Amazon Keyspaces (untuk Apache Cassandra)	`AWS::Cassandra::Keyspace`
Amazon Kinesis	`AWS::Kinesis::Stream`
AWS Lambda	`AWS::Lambda::Function`

Layanan AWS	Jenis sumber daya
Amazon MQ	`AWS::AmazonMQ::Broker`
AWS Network Firewall	`AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy`
OpenSearch Layanan Amazon	`AWS::OpenSearch::Domain`
AWS Private Certificate Authority	`AWS::ACMPCA::CertificateAuthority`
Amazon Relational Database Service	`AWS::RDS::DBCluster` , `AWS::RDS::DBClusterSnapshot` , `AWS::RDS::DBInstance` , `AWS::RDS::DBSecurityGroup` , `AWS::RDS::DBSnapshot` , `AWS::RDS::DBSubnetGroup`
Amazon Redshift	`AWS::Redshift::Cluster` , `AWS::Redshift::ClusterParameterGroup` , `AWS::Redshift::ClusterSnapshot` , `AWS::Redshift::ClusterSubnetGroup` , `AWS::Redshift::EventSubscription`
Amazon Route 53	`AWS::Route53::HealthCheck`
Amazon SageMaker AI	`AWS::SageMaker::AppImageConfig` , `AWS::SageMaker::Image`
AWS Secrets Manager	`AWS::SecretsManager::Secret`
Amazon Simple Email Service (Amazon SES)	`AWS::SES::ConfigurationSet` , `AWS::SES::ContactList`
Amazon Simple Notification Service (Amazon SNS)	`AWS::SNS::Topic`

Layanan AWS	Jenis sumber daya
Amazon Simple Queue Service (Amazon SQS)	`AWS::SQS::Queue`
AWS Step Functions	`AWS::StepFunctions::Activity`
AWS Systems Manager(SSM)	`AWS::SSM::Document`
AWS Transfer Family	`AWS::Transfer::Agreement` , `AWS::Transfer::Certificate` , `AWS::Transfer::Connector` , `AWS::Transfer::Profile` , `AWS::Transfer::Workflow`

Jadwal untuk menjalankan pemeriksaan keamanan

Setelah Anda mengaktifkan standar keamanan, AWS Security Hub CSPM mulai menjalankan semua pemeriksaan dalam waktu dua jam. Sebagian besar pemeriksaan mulai berjalan dalam waktu 25 menit. Security Hub CSPM menjalankan pemeriksaan dengan mengevaluasi aturan yang mendasari kontrol. Sampai kontrol menyelesaikan pemeriksaan pertamanya, statusnya adalah Tidak ada data.

Saat Anda mengaktifkan standar baru, CSPM Security Hub mungkin memerlukan waktu hingga 24 jam untuk menghasilkan temuan untuk kontrol yang menggunakan aturan AWS Config terkait layanan dasar yang sama dengan kontrol yang diaktifkan dari standar lain yang diaktifkan. Misalnya, jika Anda mengaktifkan Lambda.1kontrol dalam standar Praktik Terbaik Keamanan AWS Dasar (FSBP), Security Hub CSPM membuat aturan terkait layanan dan biasanya menghasilkan temuan dalam hitungan menit. Setelah ini, jika Anda mengaktifkan Lambda.1 kontrol dalam Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), mungkin diperlukan waktu hingga 24 jam bagi CSPM Security Hub untuk menghasilkan temuan untuk kontrol karena menggunakan aturan terkait layanan yang sama.

Setelah pemeriksaan awal, jadwal untuk setiap kontrol dapat berupa periodik atau perubahan yang dipicu. Untuk kontrol yang didasarkan pada AWS Config aturan terkelola, deskripsi kontrol menyertakan tautan ke deskripsi aturan di Panduan AWS Config Pengembang. Deskripsi itu menentukan apakah aturan tersebut dipicu perubahan atau periodik.

Pemeriksaan keamanan berkala

Pemeriksaan keamanan berkala berjalan secara otomatis dalam waktu 12 atau 24 jam setelah proses terbaru. Security Hub CSPM menentukan periodisitas, dan Anda tidak dapat mengubahnya. Kontrol periodik mencerminkan evaluasi pada saat pemeriksaan berjalan.

Jika Anda memperbarui status alur kerja dari temuan kontrol berkala, dan kemudian pada pemeriksaan berikutnya status kepatuhan temuan tetap sama, status alur kerja tetap dalam status yang diubah. Misalnya, jika Anda memiliki temuan gagal untuk KMS.4kontrol (AWS KMS keyrotasi harus diaktifkan), dan kemudian memulihkan temuan, Security Hub CSPM mengubah status alur kerja dari ke. `NEW` `RESOLVED` Jika Anda menonaktifkan rotasi kunci KMS sebelum pemeriksaan berkala berikutnya, status alur kerja temuan tetap ada. `RESOLVED`

Pemeriksaan yang menggunakan fungsi Lambda kustom Security Hub CSPM bersifat periodik.

Change-triggered pemeriksaan keamanan

Change-triggered pemeriksaan keamanan berjalan saat sumber daya terkait berubah status. AWS Configmemungkinkan Anda memilih antara perekaman terus menerus dari perubahan status sumber daya dan perekaman harian. Jika Anda memilih perekaman harian, AWS Config mengirimkan data konfigurasi sumber daya pada akhir setiap periode 24 jam jika ada perubahan status sumber daya. Jika tidak ada perubahan, tidak ada data yang dikirimkan. Hal ini dapat menunda pembuatan temuan CSPM Security Hub hingga periode 24 jam selesai. Terlepas dari periode perekaman yang Anda pilih, Security Hub CSPM memeriksa setidaknya sekali setiap 24 jam untuk memastikan tidak ada pembaruan sumber daya yang AWS Config terlewatkan.

Secara umum, Security Hub CSPM menggunakan aturan yang dipicu perubahan bila memungkinkan. Agar sumber daya menggunakan aturan yang dipicu perubahan, ia harus mendukung item AWS Config konfigurasi.

Menghasilkan dan memperbarui temuan kontrol

AWSSecurity Hub CSPM menghasilkan dan memperbarui temuan kontrol saat menjalankan pemeriksaan terhadap kontrol keamanan. Temuan kontrol menggunakan AWSSecurity Finding Format (ASFF).

Security Hub CSPM biasanya mengenakan biaya untuk setiap pemeriksaan keamanan untuk kontrol. Namun, jika beberapa kontrol menggunakan AWS Config aturan yang sama, CSPM Security Hub hanya mengenakan biaya sekali untuk setiap pemeriksaan terhadap aturan tersebut. Misalnya, AWS

Config `iam-password-policy` aturan ini digunakan oleh beberapa kontrol dalam standar CIS AWS Foundations Benchmark dan standar Praktik Terbaik Keamanan AWS Dasar. Setiap kali Security Hub CSPM menjalankan pemeriksaan terhadap aturan itu, itu menghasilkan temuan kontrol terpisah untuk setiap kontrol terkait, tetapi hanya mengenakan biaya sekali untuk pemeriksaan.

Jika ukuran temuan kontrol melebihi maksimum 240 KB, Security Hub CSPM menghapus `Resource.Details` objek dari temuan. Untuk kontrol yang didukung oleh AWS Config sumber daya, Anda dapat meninjau detail sumber daya menggunakan AWS Config konsol.

Topik

- Temuan kontrol konsolidasi
- Menghasilkan, memperbarui, dan mengarsipkan temuan kontrol
- Otomatisasi dan penindasan temuan kontrol
- Detail kepatuhan untuk temuan kontrol
- ProductFields rincian untuk temuan kontrol
- Tingkat keparahan untuk temuan kontrol

Temuan kontrol konsolidasi

Jika temuan kontrol konsolidasi diaktifkan untuk akun Anda, Security Hub CSPM menghasilkan satu temuan atau pembaruan pencarian untuk setiap pemeriksaan keamanan kontrol, bahkan jika kontrol berlaku untuk beberapa standar yang diaktifkan. Untuk daftar kontrol dan standar yang mereka terapkan, lihatReferensi kontrol untuk Security Hub CSPM. Kami merekomendasikan untuk mengaktifkan temuan kontrol terkonsolidasi untuk mengurangi kebisingan temuan.

Jika Anda mengaktifkan CSPM Security Hub Akun AWS sebelum 23 Februari 2023, Anda dapat mengaktifkan temuan kontrol konsolidasi dengan mengikuti petunjuk nanti di bagian ini. Jika Anda mengaktifkan CSPM Security Hub pada atau setelah 23 Februari 2023, temuan kontrol konsolidasi diaktifkan secara otomatis untuk akun Anda.

Jika Anda menggunakan integrasi CSPM Security Hub dengan AWS Organizations atau akun anggota yang diundang melalui proses undangan manual, temuan kontrol konsolidasi diaktifkan untuk akun anggota hanya jika diaktifkan untuk akun administrator. Jika fitur dinonaktifkan untuk akun administrator, itu dinonaktifkan untuk akun anggota. Perilaku ini berlaku untuk akun anggota baru dan yang sudah ada. Selain itu, jika administrator menggunakan konfigurasi pusat untuk mengelola CSPM Security Hub untuk beberapa akun, mereka tidak dapat menggunakan kebijakan konfigurasi pusat untuk mengaktifkan atau menonaktifkan temuan kontrol konsolidasi untuk akun.

Jika Anda menonaktifkan temuan kontrol konsolidasi untuk akun Anda, Security Hub CSPM akan menghasilkan atau memperbarui temuan kontrol terpisah untuk setiap standar yang diaktifkan yang menyertakan kontrol. Misalnya, jika Anda mengaktifkan empat standar yang berbagi kontrol, Anda menerima empat temuan terpisah setelah pemeriksaan keamanan untuk kontrol. Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Anda hanya menerima satu temuan.

Saat Anda mengaktifkan temuan kontrol terkonsolidasi, Security Hub CSPM menciptakan temuan agnostik standar baru dan mengarsipkan temuan berbasis standar asli. Beberapa bidang dan nilai pencarian kontrol akan berubah, yang mungkin memengaruhi alur kerja Anda yang ada. Untuk informasi tentang perubahan ini, lihatTemuan kontrol konsolidasi — Perubahan ASFF. Mengaktifkan temuan kontrol konsolidasi juga dapat memengaruhi temuan yang diterima produk pihak ketiga terintegrasi dari Security Hub CSPM. Jika Anda menggunakan Respons Keamanan Otomatis pada solusi AWS v2.0.0, perhatikan bahwa solusi ini mendukung temuan kontrol terkonsolidasi.

Untuk mengaktifkan atau menonaktifkan temuan kontrol konsolidasi, Anda harus masuk ke akun administrator atau akun mandiri.

> **Note**
>
> Setelah Anda mengaktifkan temuan kontrol terkonsolidasi, dibutuhkan waktu hingga 24 jam bagi Security Hub CSPM untuk menghasilkan temuan konsolidasi baru dan mengarsipkan temuan berbasis standar yang ada. Demikian pula, setelah menonaktifkan temuan kontrol konsolidasi, dibutuhkan waktu hingga 24 jam bagi Security Hub CSPM untuk menghasilkan temuan berbasis standar baru dan mengarsipkan temuan konsolidasi yang ada. Selama masa-masa ini, Anda mungkin melihat campuran temuan agnostik standar dan berbasis standar di akun Anda.

Security Hub CSPM console

Untuk mengaktifkan atau menonaktifkan temuan kontrol konsolidasi

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pada Pengaturan, pilih Umum.
3. Di bagian Kontrol, pilih Edit.
4. Gunakan sakelar temuan kontrol Konsolidasi untuk mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi.
5. Pilih Simpan.

Security Hub CSPM API

Untuk mengaktifkan atau menonaktifkan temuan kontrol terkonsolidasi secara terprogram, gunakan UpdateSecurityHubConfigurationpengoperasian Security Hub CSPM API. Atau, jika Anda menggunakanAWS CLI, jalankan update-security-hub-configurationperintah.

Untuk `control-finding-generator` parameter, tentukan `SECURITY_CONTROL` untuk mengaktifkan temuan kontrol terkonsolidasi. Untuk menonaktifkan temuan kontrol konsolidasi, tentukan`STANDARD_CONTROL`.

Misalnya, AWS CLI perintah berikut memungkinkan temuan kontrol terkonsolidasi.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

AWS CLIPerintah berikut menonaktifkan temuan kontrol konsolidasi.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

Menghasilkan, memperbarui, dan mengarsipkan temuan kontrol

Security Hub CSPM menjalankan pemeriksaan keamanan sesuai jadwal. Pertama kali Security Hub CSPM menjalankan pemeriksaan keamanan untuk kontrol, ini menghasilkan temuan baru untuk setiap AWS sumber daya yang diperiksa kontrol. Setiap kali Security Hub CSPM kemudian menjalankan pemeriksaan keamanan untuk kontrol, itu memperbarui temuan yang ada untuk melaporkan hasil pemeriksaan. Ini berarti Anda dapat menggunakan data yang disediakan oleh temuan individu untuk melacak perubahan kepatuhan untuk sumber daya tertentu terhadap kontrol tertentu.

Misalnya, jika status kepatuhan sumber daya berubah dari `FAILED` ke `PASSED` untuk kontrol tertentu, Security Hub CSPM tidak menghasilkan temuan baru. Sebagai gantinya, Security Hub CSPM memperbarui temuan yang ada untuk kontrol dan sumber daya. Dalam temuan tersebut, Security Hub CSPM mengubah nilai untuk bidang status kepatuhan (`Compliance.Status`) menjadi. `PASSED` Security Hub CSPM juga memperbarui nilai untuk bidang tambahan untuk mencerminkan hasil pemeriksaan—misalnya, label tingkat keparahan, status alur kerja, dan stempel waktu yang menunjukkan kapan Security Hub CSPM baru-baru ini menjalankan pemeriksaan dan memperbarui temuan.

Saat melaporkan perubahan status kepatuhan, CSPM Security Hub dapat memperbarui salah satu bidang berikut dalam temuan kontrol:

- `Compliance.Status`— Status kepatuhan baru dari sumber daya untuk kontrol yang ditentukan.
- `FindingProviderFields.Severity.Label`— Representasi kualitatif baru dari tingkat keparahan temuan, seperti`LOW`,`MEDIUM`, atau`HIGH`.
- `FindingProviderFields.Severity.Original`— Representasi kuantitatif baru dari tingkat keparahan temuan, seperti `0` untuk sumber daya yang sesuai.
- `FirstObservedAt`— Ketika status kepatuhan sumber daya baru-baru ini berubah.
- `LastObservedAt`— Ketika Security Hub CSPM baru-baru ini menjalankan pemeriksaan keamanan untuk kontrol dan sumber daya yang ditentukan.
- `ProcessedAt`— Ketika Security Hub CSPM baru-baru ini mulai memproses temuan.
- `ProductFields.PreviousComplianceStatus`— Status kepatuhan sebelumnya (`Compliance.Status`) dari sumber daya untuk kontrol yang ditentukan.
- `UpdatedAt`— Ketika Security Hub CSPM terbaru memperbarui temuan.
- `Workflow.Status`— Status investigasi terhadap temuan, berdasarkan status kepatuhan baru sumber daya untuk kontrol yang ditentukan.

Apakah Security Hub CSPM memperbarui bidang tergantung terutama pada hasil pemeriksaan keamanan terbaru untuk kontrol dan sumber daya yang berlaku. Misalnya, jika status kepatuhan sumber daya berubah dari `PASSED` ke `FAILED` untuk kontrol tertentu, CSPM Security Hub mengubah status alur kerja temuan menjadi. `NEW` Untuk melacak pembaruan temuan individu, Anda dapat merujuk ke riwayat temuan. Untuk detail tentang bidang individual dalam temuan, lihat AWSSecurity Finding Format (ASFF).

Dalam kasus tertentu, Security Hub CSPM menghasilkan temuan baru untuk pemeriksaan selanjutnya dengan kontrol, alih-alih memperbarui temuan yang ada. Ini dapat terjadi jika ada masalah dengan AWS Config aturan yang mendukung kontrol. Jika ini terjadi, Security Hub CSPM mengarsipkan temuan yang ada dan menghasilkan temuan baru untuk setiap pemeriksaan. Dalam temuan baru, status kepatuhan adalah `NOT_AVAILABLE` dan status catatan adalah`ARCHIVED`. Setelah Anda mengatasi masalah dengan AWS Config aturan, Security Hub CSPM menghasilkan temuan baru dan mulai memperbaruinya untuk melacak perubahan berikutnya pada status kepatuhan sumber daya individu.

Selain menghasilkan dan memperbarui temuan kontrol, Security Hub CSPM secara otomatis mengarsipkan temuan kontrol yang memenuhi kriteria tertentu. Security Hub CSPM mengarsipkan

temuan jika kontrol dinonaktifkan, sumber daya yang ditentukan dihapus, atau sumber daya yang ditentukan tidak ada lagi. Sumber daya mungkin tidak ada lagi karena layanan terkait tidak lagi digunakan. Lebih khusus lagi, Security Hub CSPM secara otomatis mengarsipkan temuan kontrol jika temuan tersebut memenuhi salah satu kriteria berikut:

- Temuan ini belum diperbarui selama 3-5 hari. Perhatikan bahwa arsip berdasarkan kerangka waktu ini adalah upaya terbaik dan tidak dijamin.
- AWS ConfigEvaluasi terkait dikembalikan `NOT_APPLICABLE` untuk status kepatuhan sumber daya yang ditentukan.

Untuk menentukan apakah suatu temuan diarsipkan, Anda dapat merujuk ke bidang record state (`RecordState`) dari temuan tersebut. Jika temuan diarsipkan, nilai untuk bidang ini adalah`ARCHIVED`.

Security Hub CSPM menyimpan temuan kontrol yang diarsipkan selama 30 hari. Setelah 30 hari, temuan berakhir dan Security Hub CSPM menghapusnya secara permanen. Untuk menentukan apakah temuan kontrol yang diarsipkan telah kedaluwarsa, Security Hub CSPM mendasarkan perhitungannya pada nilai untuk `UpdatedAt` bidang temuan.

Untuk menyimpan temuan kontrol yang diarsipkan selama lebih dari 30 hari, Anda dapat mengekspor temuan ke ember S3. Anda dapat melakukan ini dengan menggunakan tindakan kustom dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat Menggunakan EventBridge untuk respon otomatis dan remediasi.

> **Note**
>
> Sebelum 3 Juli 2025, Security Hub CSPM menghasilkan dan memperbarui temuan kontrol secara berbeda ketika status kepatuhan sumber daya berubah untuk kontrol. Sebelumnya, Security Hub CSPM membuat temuan kontrol baru dan mengarsipkan temuan yang ada untuk sumber daya. Oleh karena itu, Anda mungkin memiliki beberapa temuan yang diarsipkan untuk kontrol dan sumber daya tertentu sampai temuan tersebut kedaluwarsa (setelah 30 hari).

Otomatisasi dan penindasan temuan kontrol

Anda dapat menggunakan aturan otomatisasi CSPM Security Hub untuk memperbarui atau menekan temuan kontrol tertentu. Jika Anda menekan temuan, Anda dapat terus mengaksesnya.

Namun, penindasan menunjukkan keyakinan Anda bahwa tidak ada tindakan yang diperlukan untuk mengatasi temuan tersebut.

Dengan menekan temuan, Anda dapat mengurangi kebisingan temuan. Misalnya, Anda mungkin menekan temuan kontrol yang dihasilkan di akun pengujian. Atau, Anda mungkin menekan temuan yang terkait dengan sumber daya tertentu. Untuk mempelajari lebih lanjut tentang memperbarui atau menekan temuan secara otomatis, lihatMemahami aturan otomatisasi di Security Hub CSPM.

Aturan otomatisasi sesuai ketika Anda ingin memperbarui atau menekan temuan kontrol tertentu. Namun, jika kontrol tidak relevan dengan organisasi atau kasus penggunaan Anda, sebaiknya nonaktifkan kontrol. Jika Anda menonaktifkan kontrol, Security Hub CSPM tidak menjalankan pemeriksaan keamanan untuk itu dan Anda tidak dikenakan biaya untuk itu.

Detail kepatuhan untuk temuan kontrol

Dalam temuan yang dihasilkan oleh pemeriksaan keamanan untuk kontrol, objek Kepatuhan dan bidang dalam AWS Security Finding Format (ASFF) memberikan rincian kepatuhan untuk sumber daya individu yang diperiksa oleh kontrol. Ini termasuk informasi berikut:

- `AssociatedStandards`— Standar yang diaktifkan di mana kontrol diaktifkan.
- `RelatedRequirements`— Persyaratan terkait untuk kontrol di semua standar yang diaktifkan. Persyaratan ini berasal dari kerangka keamanan pihak ketiga untuk kontrol, seperti Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) atau standar NIST SP 800-171 Revisi 2.
- `SecurityControlId`— Pengidentifikasi untuk kontrol di seluruh standar yang didukung Security Hub CSPM.
- `Status`— Hasil pemeriksaan terbaru bahwa Security Hub CSPM berjalan untuk kontrol. Hasil pemeriksaan sebelumnya dipertahankan dalam sejarah temuan.
- `StatusReasons`— Array yang mencantumkan alasan untuk nilai yang ditentukan oleh `Status` bidang. Untuk setiap alasan, ini termasuk kode alasan dan deskripsi.

Tabel berikut mencantumkan kode alasan dan deskripsi bahwa temuan mungkin termasuk dalam `StatusReasons` array. Langkah-langkah remediasi bervariasi berdasarkan kontrol mana yang menghasilkan temuan dengan kode alasan tertentu. Untuk meninjau panduan remediasi untuk kontrol, lihat. Referensi kontrol untuk Security Hub CSPM

Kode alasan	Status kepatuhan	Deskripsi
`CLOUDTRAIL_METRIC_FILTER_NOT_VALID`	`FAILED`	CloudTrail Jejak Multi-wilayah tidak memiliki filter metrik yang valid.
`CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT`	`FAILED`	Filter metrik tidak ada untuk CloudTrail jejak Multi-wilayah.
`CLOUDTRAIL_MULTI_REGION_NOT_PRESENT`	`FAILED`	Akun tidak memiliki CloudTrail jejak Multi-wilayah dengan konfigurasi yang diperlukan.
`CLOUDTRAIL_REGION_INVAILD`	`WARNING`	Multi-Region CloudTrail jalur tidak ada di Wilayah saat ini.
`CLOUDWATCH_ALARM_ACTIONS_NOT_VALID`	`FAILED`	Tidak ada tindakan alarm yang valid.
`CLOUDWATCH_ALARMS_NOT_PRESENT`	`FAILED`	CloudWatch alarm tidak ada di akun.
`CONFIG_ACCESS_DENIED`	`NOT_AVAILABLE` AWS ConfigStatus adalah `ConfigError`	AWS Configakses ditolak. Verifikasi bahwa AWS Config diaktifkan dan telah diberikan izin yang cukup.
`CONFIG_EVALUATIONS_EMPTY`	`PASSED`	AWS Configmengevaluasi sumber daya Anda berdasarkan aturan. Aturan tidak berlaku untuk AWS sumber daya dalam ruang lingkupnya, sumber daya yang ditentukan dihapus, atau hasil evaluasi dihapus.
`CONFIG_RECORDER_CUSTOM_ROLE`	`FAILED`(untuk Config.1)	AWS ConfigPerekam menggunakan peran IAM khusus alih-alih peran

Kode alasan	Status kepatuhan	Deskripsi
		AWS Config terkait layanan, dan parameter `includeConfigServiceLinkedRoleCheck` khusus untuk Config.1 tidak disetel ke. `false`
`CONFIG_RECORDER_DISABLED`	`FAILED`(untuk Config.1)	AWS Configtidak diaktifkan dengan perekam konfigurasi dihidupkan.
`CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES`	`FAILED`(untuk Config.1)	AWS Configtidak merekam semua jenis sumber daya yang sesuai dengan kontrol CSPM Security Hub yang diaktifkan. Aktifkan perekaman untuk sumber daya berikut:*`Resources that aren't being recorded`*.
`CONFIG_RETURNS_NOT_APPLICABLE`	`NOT_AVAILABLE`	Status kepatuhan adalah `NOT_AVAILABLE` karena AWS Config mengembalikan status Tidak Berlaku. AWS Configtidak memberikan alasan untuk status tersebut. Berikut adalah beberapa kemungkinan alasan untuk status Tidak Berlaku: • Sumber daya telah dihapus dari ruang lingkup AWS Config aturan. • AWS ConfigAturan itu dihapus. • Sumber daya telah dihapus. • Logika AWS Config aturan dapat menghasilkan status Tidak Berlaku.

Kode alasan	Status kepatuhan	Deskripsi
`CONFIG_RULE_EVALUATION_ERROR`	`NOT_AVAILABLE` AWS ConfigStatus adalah `ConfigError`	Kode alasan ini digunakan untuk beberapa jenis kesalahan evaluasi. Deskripsi memberikan informasi alasan spesifik. Jenis kesalahan dapat berupa salah satu dari yang berikut: • Ketidakmampuan untuk melakukan evaluasi karena kurangnya izin. Deskripsi memberikan izin khusus yang hilang. • Nilai yang hilang atau tidak valid untuk parameter. Deskripsi memberikan parameter dan persyaratan untuk nilai parameter. • Kesalahan membaca dari ember S3. Deskripsi mengidentifikasi ember dan memberikan kesalahan spesifik. • AWSLangganan yang hilang. • Batas waktu umum pada evaluasi. • Akun yang ditangguhkan.
`CONFIG_RULE_NOT_FOUND`	`NOT_AVAILABLE` AWS ConfigStatus adalah `ConfigError`	AWS ConfigAturannya sedang dalam proses diciptakan.
`INTERNAL_SERVICE_ERROR`	`NOT_AVAILABLE`	Terjadi kesalahan yang tidak diketahui.

Kode alasan	Status kepatuhan	Deskripsi
`LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE`	`FAILED`	Security Hub CSPM tidak dapat melakukan pemeriksaan terhadap runtime Lambda kustom.
`S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION`	`WARNING`	Temuan ini dalam `WARNING` keadaan karena bucket S3 yang dikaitkan dengan aturan ini berada di Wilayah atau akun yang berbeda. Aturan ini tidak mendukung pemeriksaan lintas wilayah atau lintas akun. Disarankan agar Anda menonaktifkan kontrol ini di Wilayah atau akun ini. Jalankan saja di Wilayah atau akun tempat sumber daya berada.
`SNS_SUBSCRIPTION_NOT_PRESENT`	`FAILED`	Filter metrik CloudWatch Log tidak memiliki langganan Amazon SNS yang valid.
`SNS_TOPIC_CROSS_ACCOUNT`	`WARNING`	Temuan itu dalam `WARNING` keadaan. Topik SNS yang terkait dengan aturan ini dimiliki oleh akun yang berbeda. Akun saat ini tidak dapat memperoleh informasi berlangganan. Akun yang memiliki topik SNS harus memberikan `sns:ListSubscriptionsByTopic` izin kepada akun saat ini untuk topik SNS.

Kode alasan	Status kepatuhan	Deskripsi
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	Temuan ini dalam WARNING keadaan karena topik SNS yang terkait dengan aturan ini berada di Wilayah atau akun yang berbeda. Aturan ini tidak mendukung pemeriksaan lintas wilayah atau lintas akun. Disarankan agar Anda menonaktifkan kontrol ini di Wilayah atau akun ini. Jalankan saja di Wilayah atau akun tempat sumber daya berada.
SNS_TOPIC_INVALID	FAILED	Topik SNS yang terkait dengan aturan ini tidak valid.
THROTTLING_ERROR	NOT_AVAILABLE	Operasi API yang relevan melebihi tarif yang diizinkan.

ProductFields rincian untuk temuan kontrol

Dalam temuan yang dihasilkan oleh pemeriksaan keamanan untuk kontrol, ProductFieldsatribut dalam AWS Security Finding Format (ASFF) dapat menyertakan bidang berikut.

`ArchivalReasons:0/Description`

Menjelaskan mengapa Security Hub CSPM mengarsipkan temuan.

Misalnya, CSPM Security Hub mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar, atau Anda mengaktifkan atau menonaktifkan temuan kontrol konsolidasi.

`ArchivalReasons:0/ReasonCode`

Menentukan mengapa Security Hub CSPM mengarsipkan temuan.

Misalnya, CSPM Security Hub mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar, atau Anda mengaktifkan atau menonaktifkan temuan kontrol konsolidasi.

`PreviousComplianceStatus`

Status kepatuhan sebelumnya (`Compliance.Status`) dari sumber daya untuk kontrol yang ditentukan, pada pembaruan terbaru untuk temuan. Jika status kepatuhan sumber daya tidak berubah selama pembaruan terbaru, nilai ini sama dengan nilai untuk `Compliance.Status` bidang temuan. Untuk daftar peluang nilai, lihat Mengevaluasi status kepatuhan dan status kontrol.

`StandardsGuideArn` atau `StandardsArn`

ARN standar yang terkait dengan kontrol.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah. `StandardsGuideArn` Untuk standar PCI DSS dan AWS Foundational Security Best Practices, bidangnya adalah. `StandardsArn`

Bidang ini dihapus demi `Compliance.AssociatedStandards` jika Anda mengaktifkan temuan kontrol terkonsolidasi.

`StandardsGuideSubscriptionArn` atau `StandardsSubscriptionArn`

ARN berlangganan akun ke standar.

Untuk standar CIS AWS Foundations Benchmark, bidangnya adalah. `StandardsGuideSubscriptionArn` Untuk standar PCI DSS dan AWS Foundational Security Best Practices, bidangnya adalah. `StandardsSubscriptionArn`

Bidang ini dihapus jika Anda mengaktifkan temuan kontrol konsolidasi.

`RuleId` atau `ControlId`

Pengidentifikasi untuk kontrol.

Untuk versi 1.2.0 dari standar AWS CIS Foundations Benchmark, bidangnya adalah. `RuleId` Untuk standar lain, termasuk versi berikutnya dari standar CIS AWS Foundations Benchmark, bidangnya adalah. `ControlId`

Bidang ini dihapus demi `Compliance.SecurityControlId` jika Anda mengaktifkan temuan kontrol terkonsolidasi.

`RecommendationUrl`

URL untuk informasi remediasi untuk kontrol. Bidang ini dihapus demi `Remediation.Recommendation.Url` jika Anda mengaktifkan temuan kontrol terkonsolidasi.

`RelatedAWSResources:0/name`

Nama sumber daya yang terkait dengan temuan.

`RelatedAWSResource:0/type`

Jenis sumber daya yang terkait dengan kontrol.

`StandardsControlArn`

ARN kontrol. Bidang ini dihapus jika Anda mengaktifkan temuan kontrol konsolidasi.

`aws/securityhub/ProductName`

Untuk temuan kontrol, nama produknya adalah`Security Hub`.

`aws/securityhub/CompanyName`

Untuk temuan kontrol, nama perusahaan adalah`AWS`.

`aws/securityhub/annotation`

Deskripsi masalah yang ditemukan oleh kontrol.

`aws/securityhub/FindingId`

Pengidentifikasi untuk temuan.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol terkonsolidasi.

Tingkat keparahan untuk temuan kontrol

Tingkat keparahan yang ditetapkan ke kontrol CSPM Security Hub menunjukkan pentingnya kontrol. Tingkat keparahan kontrol menentukan label keparahan yang ditetapkan untuk temuan kontrol.

Kriteria keparahan

Tingkat keparahan kontrol ditentukan berdasarkan penilaian kriteria berikut:

- Seberapa sulit bagi aktor ancaman untuk memanfaatkan kelemahan konfigurasi yang terkait dengan kontrol? Kesulitan ditentukan oleh jumlah kecanggihan atau kompleksitas yang diperlukan untuk menggunakan kelemahan untuk melakukan skenario ancaman.

- Seberapa besar kemungkinan kelemahan itu akan mengarah pada kompromi Akun AWS atau sumber daya Anda? Kompromi terhadap sumber daya Anda Akun AWS berarti kerahasiaan, integritas, atau ketersediaan data atau AWS infrastruktur Anda rusak dalam beberapa cara. Kemungkinan kompromi menunjukkan seberapa besar kemungkinan skenario ancaman akan mengakibatkan gangguan atau pelanggaran sumber daya Anda Layanan AWS atau sumber daya.

Sebagai contoh, pertimbangkan kelemahan konfigurasi berikut:

- Kunci akses pengguna tidak diputar setiap 90 hari.
- Kunci pengguna root IAM ada.

Kedua kelemahan sama-sama sulit untuk dimanfaatkan musuh. Dalam kedua kasus, musuh dapat menggunakan pencurian kredenal atau metode lain untuk memperoleh kunci pengguna. Mereka kemudian dapat menggunakannya untuk mengakses sumber daya Anda dengan cara yang tidak sah.

Namun, kemungkinan kompromi jauh lebih tinggi jika aktor ancaman memperoleh kunci akses pengguna root karena ini memberi mereka akses yang lebih besar. Akibatnya, kelemahan kunci pengguna root memiliki tingkat keparahan yang lebih tinggi.

Tingkat keparahannya tidak memperhitungkan kekritisan sumber daya yang mendasarinya. Kekritisan adalah tingkat pentingnya sumber daya yang terkait dengan temuan tersebut. Misalnya, sumber daya yang terkait dengan aplikasi kritis misi lebih penting daripada sumber daya yang terkait dengan pengujian non-produksi. Untuk menangkap informasi kekritisan sumber daya, gunakan `Criticality` bidang AWS Security Finding Format (ASFF).

Tabel berikut memetakan kesulitan untuk mengeksploitasi dan kemungkinan kompromi dengan label keamanan.

	Kompromi sangat mungkin	Kemungkinan kompromi	Kompromi tidak mungkin	Kompromi sangat tidak mungkin
Sangat mudah dieksploitasi	Kritis	Kritis	Tinggi	Sedang
Agak mudah dieksploitasi	Kritis	Tinggi	Sedang	Sedang

Agak sulit untuk dieksploitasi	Tinggi	Sedang	Sedang	Rendah
Sangat sulit untuk dieksploi tasi	Sedang	Sedang	Rendah	Rendah

Definisi keparahan

Label keparahan didefinisikan sebagai berikut.

Kritis — Masalah ini harus segera diperbaiki untuk menghindari eskalasi.

Misalnya, bucket S3 terbuka dianggap sebagai temuan tingkat keparahan kritis. Karena begitu banyak pelaku ancaman memindai bucket S3 terbuka, data dalam bucket S3 yang terbuka kemungkinan akan ditemukan dan diakses oleh orang lain.

Secara umum, sumber daya yang dapat diakses publik dianggap sebagai masalah keamanan kritis. Anda harus memperlakukan temuan kritis dengan sangat mendesak. Anda juga harus mempertimbangkan kekritisan sumber daya.

Tinggi — Masalah ini harus ditangani sebagai prioritas jangka pendek.

Misalnya, jika grup keamanan VPC default terbuka untuk lalu lintas masuk dan keluar, itu dianggap tingkat keparahan yang tinggi. Agak mudah bagi aktor ancaman untuk mengkompromikan VPC menggunakan metode ini. Kemungkinan juga aktor ancaman akan dapat mengganggu atau mengeksfiltrasi sumber daya begitu mereka berada di VPC.

Security Hub CSPM merekomendasikan agar Anda memperlakukan temuan tingkat keparahan tinggi sebagai prioritas jangka pendek. Anda harus segera mengambil langkah-langkah remediasi. Anda juga harus mempertimbangkan kekritisan sumber daya.

Medium — Masalah ini harus ditangani sebagai prioritas jangka menengah.

Misalnya, kurangnya enkripsi untuk data dalam perjalanan dianggap sebagai temuan tingkat keparahan sedang. Dibutuhkan serangan man-in-the-middle yang canggih untuk memanfaatkan kelemahan ini. Dengan kata lain, ini agak sulit. Kemungkinan beberapa data akan dikompromikan jika skenario ancaman berhasil.

Security Hub CSPM merekomendasikan agar Anda menyelidiki sumber daya yang terlibat secepat mungkin. Anda juga harus mempertimbangkan kekritisan sumber daya.

Rendah — Masalah ini tidak memerlukan tindakan sendiri.

Misalnya, kegagalan untuk mengumpulkan informasi forensik dianggap tingkat keparahan rendah. Kontrol ini dapat membantu mencegah kompromi di masa depan, tetapi tidak adanya forensik tidak mengarah langsung pada kompromi.

Anda tidak perlu mengambil tindakan segera pada temuan tingkat keparahan rendah, tetapi mereka dapat memberikan konteks ketika Anda menghubungkannya dengan masalah lain.

Informasi - Tidak ada kelemahan konfigurasi yang ditemukan.

Dengan kata lain, statusnya adalah`PASSED`,`WARNING`, atau`NOT AVAILABLE`.

Tidak ada tindakan yang disarankan. Temuan informasi membantu pelanggan untuk menunjukkan bahwa mereka berada dalam keadaan patuh.

Mengevaluasi status kepatuhan dan status kontrol

`Compliance.Status`Bidang Format Pencarian AWS Keamanan menjelaskan hasil temuan kontrol. AWSSecurity Hub CSPM menggunakan status kepatuhan temuan kontrol untuk menentukan status kontrol secara keseluruhan. Status kontrol ditampilkan pada halaman detail kontrol pada konsol CSPM Security Hub.

Mengevaluasi status kepatuhan temuan CSPM Security Hub

Status kepatuhan untuk setiap temuan diberikan salah satu dari nilai berikut:

- `PASSED`— Menunjukkan bahwa kontrol melewati pemeriksaan keamanan untuk temuan tersebut. Ini secara otomatis mengatur CSPM `Workflow.Status` Security Hub ke. `RESOLVED`
- `FAILED`— Menunjukkan bahwa kontrol tidak lulus pemeriksaan keamanan untuk temuan tersebut.
- `WARNING`— Menunjukkan bahwa Security Hub CSPM tidak dapat menentukan apakah sumber daya berada dalam status `PASSED` atau `FAILED` tidak. Misalnya, perekaman AWS Config sumber daya tidak diaktifkan untuk jenis sumber daya yang sesuai.
- `NOT_AVAILABLE`— Menunjukkan bahwa pemeriksaan tidak dapat diselesaikan karena server gagal, sumber daya dihapus, atau hasil AWS Config evaluasi`NOT_APPLICABLE`. Jika hasil AWS Config evaluasi itu`NOT_APPLICABLE`, Security Hub CSPM secara otomatis mengarsipkan temuan tersebut.

Jika status kepatuhan untuk temuan berubah dari PASSED menjadi,, atau FAILEDWARNING, dan Workflow.Status merupakan salah satu NOTIFIED atau NOT_AVAILABLERESOLVED, CSPM Security Hub secara otomatis berubah Workflow.Status menjadi. NEW

Jika Anda tidak memiliki sumber daya yang sesuai dengan kontrol, Security Hub CSPM menghasilkan PASSED temuan di tingkat akun. Jika Anda memiliki sumber daya yang sesuai dengan kontrol tetapi kemudian menghapus sumber daya, Security Hub CSPM membuat NOT_AVAILABLE temuan dan mengarsipkannya segera. Setelah 18 jam, Anda menerima PASSED temuan karena Anda tidak lagi memiliki sumber daya yang sesuai dengan kontrol.

Mendapatkan status kontrol dari status kepatuhan

Security Hub CSPM memperoleh status kontrol keseluruhan dari status kepatuhan temuan kontrol. Saat menentukan status kontrol, Security Hub CSPM mengabaikan temuan yang memiliki RecordState of ARCHIVED dan temuan yang memiliki a of. Workflow.Status SUPPRESSED

Status kontrol diberikan salah satu nilai berikut:

- Lulus — Menunjukkan bahwa semua temuan memiliki status kepatuhanPASSED.
- Gagal - Menunjukkan bahwa setidaknya satu temuan memiliki status kepatuhanFAILED.
- Tidak diketahui - Menunjukkan bahwa setidaknya satu temuan memiliki status kepatuhan WARNING atauNOT_AVAILABLE. Tidak ada temuan yang memiliki status kepatuhanFAILED.
- Tidak ada data — Menunjukkan bahwa tidak ada temuan untuk kontrol. Misalnya, kontrol yang baru diaktifkan memiliki status ini sampai Security Hub CSPM mulai menghasilkan temuan untuk itu. Kontrol juga memiliki status ini jika semua temuannya SUPPRESSED atau tidak tersedia saat iniWilayah AWS.
- Dinonaktifkan - Menunjukkan bahwa kontrol dinonaktifkan di akun saat ini dan Wilayah. Saat ini tidak ada pemeriksaan keamanan yang dilakukan untuk kontrol ini di akun saat ini dan Wilayah. Namun, temuan kontrol yang dinonaktifkan mungkin memiliki nilai untuk status kepatuhan hingga 24 jam setelah penonaktifan.

Untuk akun administrator, status kontrol mencerminkan status kontrol untuk akun administrator dan akun anggota. Secara khusus, status keseluruhan kontrol muncul sebagai Gagal jika kontrol memiliki satu atau lebih temuan gagal di akun administrator atau salah satu akun anggota. Jika Anda telah menetapkan Wilayah agregasi, status kontrol di Wilayah agregasi mencerminkan status kontrol di Wilayah agregasi dan Wilayah yang ditautkan. Secara khusus, status keseluruhan kontrol muncul

sebagai Gagal jika kontrol memiliki satu atau lebih temuan gagal di Wilayah agregasi atau salah satu Wilayah terkait.

Security Hub CSPM biasanya menghasilkan status kontrol awal dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ringkasan atau halaman standar Keamanan di konsol CSPM Security Hub. Anda harus memiliki perekaman AWS Config sumber daya yang dikonfigurasi agar status kontrol muncul. Setelah status kontrol dibuat untuk pertama kalinya, Security Hub CSPM memperbarui status kontrol setiap 24 jam berdasarkan temuan dari 24 jam sebelumnya. Stempel waktu pada halaman detail kontrol menunjukkan kapan status kontrol terakhir diperbarui.

> **Note**
>
> Setelah mengaktifkan kontrol untuk pertama kalinya, diperlukan waktu hingga 24 jam untuk status kontrol yang akan dihasilkan di Wilayah Tiongkok dan. AWS GovCloud (US) Region

Menghitung skor keamanan

Pada konsol CSPM AWS Security Hub, halaman Ring kasan dan halaman Kontrol menampilkan skor keamanan ringkasan di semua standar yang diaktifkan. Pada halaman Standar keamanan, Security Hub CSPM juga menampilkan skor keamanan dari 0-100 persen untuk setiap standar yang diaktifkan.

Saat pertama kali mengaktifkan Security Hub CSPM, Security Hub CSPM menghitung skor keamanan ringkasan dan skor keamanan standar dalam waktu 30 menit setelah kunjungan pertama Anda ke halaman Ring kasan atau Standar Keamanan di konsol. Skor dibuat hanya untuk standar yang diaktifkan saat Anda mengunjungi halaman tersebut di konsol. Selain itu, perekaman AWS Config sumber daya harus dikonfigurasi agar skor muncul. Skor keamanan ringkasan adalah rata-rata skor keamanan standar. Untuk meninjau daftar standar yang saat ini diaktifkan, Anda dapat menggunakan pen GetEnabledStandards goperasian Security Hub CSPM API.

Setelah pembuatan skor pertama kali, Security Hub CSPM memperbarui skor keamanan setiap 24 jam. Security Hub CSPM menampilkan stempel waktu untuk menunjukkan kapan skor keamanan terakhir diperbarui. Perhatikan bahwa skor keamanan pertama kali dapat dihasilkan di Wilayah China dan AWS GovCloud (US) Regions.

Jika Anda mengaktifkan temuan kontrol konsolidasi, skor keamanan dapat diperbarui hingga 24 jam. Selain itu, mengaktifkan Wilayah agregasi baru atau memperbarui Wilayah tertaut akan mengatur

ulang skor keamanan yang ada. Diperlukan waktu hingga 24 jam bagi Security Hub CSPM untuk menghasilkan skor keamanan baru yang mencakup data dari Wilayah yang diperbarui.

Metode penghitungan skor keamanan

Skor keamanan mewakili proporsi kontrol yang dil ewati ke kontrol yang diaktifkan. Skor ditampilkan sebagai persentase yang dibulatkan ke atas atau ke bawah ke bilangan bulat terdekat.

Security Hub CSPM menghitung skor keamanan ringkasan di semua standar yang diaktifkan. Security Hub CSPM juga menghitung skor keamanan untuk setiap standar yang diaktifkan. Untuk tujuan perhitungan skor, kontrol yang diaktifkan mencakup kontrol dengan status Lulus, Gagal, dan Tidak Diket ahui. Kontrol dengan status Tidak ada data yang dik ecualikan dari perhitungan skor.

Security Hub CSPM mengabaikan temuan yang diarsipkan dan ditekan saat menghitung status kontrol. Hal ini dapat mempengaruhi skor keamanan. Misalnya, jika Anda menekan semua temuan yang gagal untuk suatu kontrol, statusnya menjadi L ulus, yang pada gilirannya dapat meningkatkan skor keamanan Anda. Untuk informasi selengkapnya tentang status kontrol, lihatMengevaluasi status kepatuhan dan status kontrol.

Contoh penilaian:

Standar	Kontrol yang lulus	Kontrol gagal	Kontrol tidak dikenal	Skor standar
AWS Praktik Terbaik Keamanan Dasar v1.0.0	168	22	0	88%
Benchmark AWS Yayasan CIS v1.4.0	8	29	0	22%
Benchmark AWS Yayasan CIS v1.2.0	6	35	0	15%
Publikasi Khusus NIST 800-53 Revisi 5	159	56	0	74%

Standar	Kontrol yang lulus	Kontrol gagal	Kontrol tidak dikenal	Skor standar
PCI DSS v3.2.1	28	17	0	62%

Saat menghitung skor keamanan ringkasan, Security Hub CSPM menghitung setiap kontrol hanya sekali di seluruh standar. Misalnya, jika Anda telah mengaktifkan kontrol yang berlaku untuk tiga standar yang diaktifkan, kontrol tersebut hanya dihitung sebagai satu kontrol yang diaktifkan untuk tujuan penilaian.

Dalam contoh ini, meskipun jumlah total kontrol yang diaktifkan di seluruh standar yang diaktifkan adalah 528, Security Hub CSPM menghitung setiap kontrol unik hanya sekali untuk tujuan penilaian. Jumlah kontrol unik yang diaktifkan kemungkinan lebih rendah dari 528. Jika kita mengasumsikan jumlah kontrol unik yang diaktifkan adalah 515, dan jumlah kontrol unik yang dilewati adalah 357, skor ringkasan adalah 69%. Skor ini dihitung dengan membagi jumlah kontrol unik yang dilewati dengan jumlah kontrol unik yang diaktifkan.

Anda mungkin memiliki skor ringkasan yang berbeda dari skor keamanan standar, bahkan jika Anda hanya mengaktifkan satu standar di akun Anda di Wilayah saat ini. Hal ini dapat terjadi jika Anda masuk ke akun administrator dan akun anggota memiliki standar tambahan atau standar yang berbeda diaktifkan. Hal ini juga dapat terjadi jika Anda melihat skor dari Wilayah agregasi dan standar tambahan atau standar yang berbeda diaktifkan di Wilayah yang ditautkan.

Skor keamanan untuk akun administrator

Jika Anda masuk ke akun administrator, skor keamanan ringkasan dan skor standar memperhitungkan status kontrol di akun administrator dan semua akun anggota.

Jika status kontrol adalah Gagal bahkan dalam satu akun anggota, statusnya adalah Gag al di akun administrator dan memengaruhi skor akun administrator.

Jika Anda masuk ke akun administrator dan melihat skor di Wilayah agregasi, skor keamanan memperhitungkan status kontrol di semua akun anggota dan semua Wilayah yang ditautkan.

Skor keamanan jika Anda telah menetapkan Wilayah agregasi

Jika Anda telah menetapkan agregasi Wilayah AWS, skor keamanan ringkasan dan skor standar memperhitungkan status kontrol di semua
Wilayah yang terhubung.

Jika status kontrol adalah Gagal bahkan di satu Wilayah tertaut, statusnya Gagal di Wilayah agregasi dan berdampak pada skor Wilayah agregasi.

Jika Anda masuk ke akun administrator dan melihat skor di Wilayah agregasi, skor keamanan memperhitungkan status kontrol di semua akun anggota dan semua Wilayah yang ditautkan.

Kategori kontrol di Security Hub CSPM

Setiap kontrol diberi kategori. Kategori untuk kontrol mencerminkan fungsi keamanan yang berlaku untuk kontrol.

Nilai kategori berisi kategori, subkategori dalam kategori, dan, secara opsional, pengklasifikasi dalam subkategori. Contoh:

- Identifikasi > Inventaris
- Lindungi > Perlindungan data > Enkripsi data dalam perjalanan

Berikut adalah deskripsi dari kategori, subkategori, dan pengklasifikasi yang tersedia.

Identifikasi

Mengembangkan pemahaman organisasi untuk mengelola risiko keamanan siber terhadap sistem, aset, data, dan kemampuan.

Inventaris

Sudahkah layanan menerapkan strategi penandaan sumber daya yang benar? Apakah strategi penandaan termasuk pemilik sumber daya?

Sumber daya apa yang digunakan layanan ini? Apakah mereka menyetujui sumber daya untuk layanan ini?

Apakah Anda memiliki visibilitas ke inventaris yang disetujui? Misalnya, apakah Anda menggunakan layanan seperti Amazon EC2 Systems Manager dan Service Catalog?

Pencatatan log

Sudahkah Anda mengaktifkan semua pencatatan yang relevan untuk layanan ini dengan aman? Contoh file log meliputi yang berikut ini:

- Log Aliran VPC Amazon
- Log akses Elastic Load Balancing

- CloudFront Log Amazon
- CloudWatch Log Amazon
- Pencatatan Layanan Basis Data Relasional Amazon
- Log indeks lambat OpenSearch Layanan Amazon
- X-Ray menelusuri
- AWS Directory Servicelog
- AWS Configbarang
- Snapshot

Lindungi

Mengembangkan dan menerapkan perlindungan yang tepat untuk memastikan penyampaian layanan infrastruktur penting dan praktik pengkodean yang aman.

Manajemen akses yang aman

Apakah layanan menggunakan praktik hak istimewa paling sedikit dalam IAM atau kebijakan sumber dayanya?

Apakah kata sandi dan rahasia cukup kompleks? Apakah mereka diputar dengan tepat?

Apakah layanan menggunakan otentikasi multi-faktor (MFA)?

Apakah layanan menghindari pengguna root?

Apakah kebijakan berbasis sumber daya memungkinkan akses publik?

Konfigurasi jaringan aman

Apakah layanan menghindari akses jaringan jarak jauh publik dan tidak aman?

Apakah layanan menggunakan VPC dengan benar? Misalnya, apakah pekerjaan diperlukan untuk berjalan di VPC?

Apakah layanan mengelompokkan dan mengisolasi sumber daya sensitif dengan benar?

Perlindungan data

Enkripsi data saat istirahat — Apakah layanan mengenkripsi data saat istirahat?

Enkripsi data dalam perjalanan — Apakah layanan mengenkripsi data dalam perjalanan?

Integritas data — Apakah layanan memvalidasi data untuk integritas?

Perlindungan penghapusan data — Apakah layanan melindungi data dari penghapusan yang tidak disengaja?

Pengelolaan/penggunaan data — Apakah Anda menggunakan layanan seperti Amazon Macie untuk melacak lokasi data sensitif Anda?

Perlindungan API

Apakah layanan digunakan AWS PrivateLink untuk melindungi operasi API layanan?

Layanan pelindung

Apakah layanan perlindungan yang benar ada? Apakah mereka memberikan jumlah pertanggungan yang benar?

Layanan pelindung membantu Anda menangkis serangan dan kompromi yang diarahkan pada layanan. Contoh layanan perlindungan AWS termasukAWS Control Tower,,, Vanta AWS WAFAWS Shield Advanced, Secrets Manager, IAM Access Analyzer, dan. AWS Resource Access Manager

Pengembangan yang aman

Apakah Anda menggunakan praktik pengkodean yang aman?

Apakah Anda menghindari kerentanan seperti Open Web Application Security Project (OWASP) Top Ten?

Mendeteksi

Mengembangkan dan menerapkan kegiatan yang sesuai untuk mengidentifikasi terjadinya peristiwa keamanan siber.

Layanan deteksi

Apakah layanan deteksi yang benar ada?

Apakah mereka memberikan jumlah pertanggungan yang benar?

Contoh layanan AWS deteksi termasuk Amazon GuardDuty, AWS Security Hub CSPM, Amazon Inspector, Amazon Detective CloudWatch , Amazon AWS IoT Device Defender Alarm, dan. AWS Trusted Advisor

Menanggapi

Mengembangkan dan menerapkan kegiatan yang sesuai untuk mengambil tindakan terkait peristiwa keamanan siber yang terdeteksi.

Tindakan respons

- Apakah Anda menanggapi peristiwa keamanan dengan cepat?
- Apakah Anda memiliki temuan kritis atau tingkat keparahan tinggi yang aktif?

Forensik

- Bisakah Anda memperoleh data forensik dengan aman untuk layanan ini? Misalnya, apakah Anda memperoleh snapshot Amazon EBS yang terkait dengan temuan positif sejati?
- Sudahkah Anda membuat akun forensik?

Memulihkan

Mengembangkan dan mengimplementasikan kegiatan yang sesuai untuk mempertahankan rencana ketahanan dan memulihkan kemampuan atau layanan apa pun yang terganggu karena peristiwa keamanan siber.

Ketahanan

- Apakah konfigurasi layanan mendukung kegagalan yang anggun, penskalaan elastis, dan ketersediaan tinggi?
- Sudahkah Anda membuat cadangan?

Meninjau detail kontrol di Security Hub CSPM

Memilih kontrol pada halaman Kontrol atau halaman detail standar konsol CSPM Hub Keamanan membawa Anda ke halaman detail kontrol.

Bagian atas halaman detail kontrol menunjukkan status kontrol. Status kontrol merangkum kinerja kontrol berdasarkan status kepatuhan dari temuan kontrol. Security Hub CSPM biasanya menghasilkan status kontrol awal dalam waktu 30 menit setelah kunjungan pertama Anda ke

halaman Ring kasan atau halaman Standar Keamanan di konsol CSPM Hub Keamanan. Status hanya tersedia untuk kontrol yang diaktifkan saat Anda mengunjungi halaman tersebut.

Halaman detail kontrol juga memberikan rincian status kepatuhan dari temuan kontrol selama 24 jam terakhir. Untuk informasi selengkapnya tentang status kontrol dan status kepatuhan, lihatMengevaluasi status kepatuhan dan status kontrol.

AWS Config perekaman sumber daya harus dikonfigurasi agar status kontrol muncul. Setelah status kontrol dibuat untuk pertama kalinya, Security Hub CSPM memperbarui status kontrol setiap 24 jam berdasarkan temuan dari 24 jam sebelumnya.

Akun administrator melihat status kontrol agregat di seluruh akun administrator dan akun anggota. Jika Anda telah menetapkan Wilayah agregasi, status kontrol mencakup temuan di semua Wilayah yang ditautkan. Untuk informasi selengkapnya tentang status kontrol, lihatthe section called “Status kepatuhan dan status kontrol”.

Anda juga dapat mengaktifkan atau menonaktifkan kontrol dari halaman detail kontrol.

> **Note**
>
> Diperlukan waktu hingga 24 jam setelah mengaktifkan kontrol untuk status kontrol pertama kali yang akan dihasilkan di Wilayah China dan. AWS GovCloud (US) Regions

Tab Standar dan Persyaratan mencantumkan standar yang dapat diaktifkan kontrol dan persyaratan yang terkait dengan kontrol dari kerangka kepatuhan yang berbeda.

Tab Pemeriksaan mencantumkan temuan aktif untuk kontrol selama 24 jam terakhir. Temuan kontrol dihasilkan dan diperbarui saat Security Hub CSPM menjalankan pemeriksaan keamanan untuk kontrol. Daftar pada tab ini tidak menyertakan temuan yang diarsipkan.

Untuk setiap temuan, daftar menyediakan akses untuk menemukan detail seperti status kepatuhan dan sumber daya terkait. Anda juga dapat mengatur status alur kerja setiap temuan dan mengirim temuan ke tindakan khusus. Untuk informasi selengkapnya, lihat Meninjau dan mengelola temuan kontrol.

Melihat detail untuk kontrol

Pilih metode akses pilihan Anda, dan ikuti langkah-langkah ini untuk meninjau detail kontrol. Rincian berlaku untuk akun saat ini dan Wilayah dan termasuk yang berikut:

- Judul dan deskripsi kontrol.
- Tautan ke panduan remediasi untuk temuan kontrol yang gagal.
- Tingkat keparahan kontrol.
- Status kontrol.

Di konsol, Anda juga dapat meninjau daftar temuan terbaru untuk kontrol. Untuk melakukan ini secara terprogram, Anda dapat menggunakan pen GetFindings goperasian Security Hub CSPM API.

Security Hub CSPM console

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pilih Kontrol di panel navigasi.
3. Pilih kontrol.

Security Hub CSPM API

1. J `ListSecurityControlDefinitions` alankan, dan berikan satu atau lebih ARN standar untuk mendapatkan daftar ID kontrol untuk standar tersebut. Untuk mendapatkan ARN standar, jalankan `DescribeStandards`. Jika Anda tidak memberikan ARN standar, API ini mengembalikan semua ID kontrol CSPM Security Hub. API ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol berbasis standar yang ada sebelum rilis fitur ini.

   Contoh permintaan:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. J `BatchGetSecurityControls` alankan untuk mendapatkan detail tentang satu atau lebih kontrol di Akun AWS dan saat ini Wilayah AWS.

   Contoh permintaan:

   ```
   {
       "SecurityControlIds": ["Config.1", "IAM.1"]
   }
   ```

AWS CLI

1. Jalan `list-security-control-definitions` kan perintah, dan berikan satu atau lebih ARN standar untuk mendapatkan daftar ID kontrol. Untuk mendapatkan ARN standar, jalankan `describe-standards` perintah. Jika Anda tidak memberikan ARN standar, perintah ini mengembalikan semua ID kontrol CSPM Security Hub. Perintah ini mengembalikan ID kontrol keamanan agnostik standar, bukan ID kontrol berbasis standar yang ada sebelum rilis fitur ini.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Jalan `batch-get-security-controls` kan perintah untuk mendapatkan detail tentang satu atau lebih kontrol di Akun AWS dan saat ini Wilayah AWS.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-
control-ids '["Config.1", "IAM.1"]'
```

Kontrol penyaringan dan penyortiran di Security Hub CSPM

Pada konsol CSPM AWS Security Hub, Anda dapat menggunakan halaman Kontrol untuk meninjau tabel kontrol yang tersedia saat ini. Wilayah AWS Pengecualiannya adalah Wilayah agregasi. Jika Anda mengonfigurasi Wilayah agregasi dan masuk ke Wilayah tersebut, konsol menampilkan kontrol yang tersedia di Wilayah agregasi atau satu atau beberapa Wilayah tertaut.

Untuk fokus pada subset kontrol tertentu, Anda dapat mengurutkan dan memfilter tabel kontrol. Opsi Filter berdasarkan di sebelah tabel dapat membantu Anda dengan cepat fokus pada subset tertentu ini:

- Semua kontrol yang diaktifkan, yang merupakan kontrol yang diaktifkan di setidaknya satu standar yang diaktifkan.
- Semua kontrol yang dinonaktifkan, yang merupakan kontrol yang dinonaktifkan di semua standar.
- Semua kontrol yang diaktifkan yang memiliki status kontrol tertentu, seperti Gagal. Opsi Tidak ada data hanya menampilkan kontrol yang saat ini tidak memiliki temuan. Untuk informasi tentang status kontrol, lihatMengevaluasi status kepatuhan dan status kontrol.

Selain opsi Filter berdasarkan, Anda dapat memfilter tabel dengan memasukkan kriteria filter di kotak kontrol Filter di atas tabel. Misalnya, Anda dapat memfilter berdasarkan ID kontrol atau tingkat keparahan.

Secara default, kontrol dengan status Gagal dicantumkan terlebih dahulu, dalam urutan menurun berdasarkan tingkat keparahan. Anda dapat mengubah urutan pengurutan dengan memilih judul kolom yang berbeda.

> **Tip**
>
> Jika Anda memiliki alur kerja otomatis berdasarkan temuan kontrol, sebaiknya gunakan bidang `SecurityControlId` atau `SecurityControlArn` ASFF sebagai filter, bukan bidang or`Title`. `Description` Bidang terakhir dapat berubah sesekali, sedangkan ID kontrol dan ARN adalah pengidentifikasi statis.

Jika Anda masuk ke akun administrator CSPM Security Hub, kontrol yang diaktifkan menyer takan kontrol yang diaktifkan di setidaknya satu akun anggota. Jika Anda mengonfigurasi Wilayah agregasi, kontrol yang diaktifkan menyertakan kontrol yang diaktifkan di setidaknya satu Wilayah tertaut.

Jika Anda memilih opsi di samping kontrol yang diaktifkan, panel muncul dan menampilkan standar di mana kontrol saat ini diaktifkan. Anda juga dapat melihat standar di mana kontrol saat ini dinonaktifkan. Dari panel ini, Anda dapat menonaktifkan kontrol di semua standar. Untuk informasi selengkapnya, lihat Menonaktifkan kontrol di Security Hub CSPM. Untuk akun administrator, informasi di panel mencerminkan pengaturan untuk semua akun anggota Anda.

Untuk mengambil daftar kontrol secara terprogram, Anda dapat menggunakan ListSecurityControlDefinitions operasi Security Hub CSPM API. Untuk mengambil rincian kontrol individu, gunakan BatchGetSecurityControls operasi.

Memahami parameter kontrol di Security Hub CSPM

Beberapa kontrol di AWS Security Hub CSPM menggunakan parameter yang memengaruhi cara kontrol dievaluasi. Biasanya, kontrol tersebut dievaluasi terhadap nilai parameter default yang ditetapkan oleh Security Hub CSPM. Namun, untuk subset kontrol ini, Anda dapat memodifikasi nilai parameter. Saat Anda mengubah nilai parameter kontrol, Security Hub CSPM mulai mengevaluasi kontrol terhadap nilai yang Anda tentukan. Jika sumber daya yang mendasari kontrol memenuhi nilai kustom, Security Hub CSPM menghasilkan temuan. `PASSED` Jika sumber daya tidak memenuhi nilai kustom, Security Hub CSPM menghasilkan temuan. `FAILED`

Dengan menyesuaikan parameter kontrol, Anda dapat menyempurnakan praktik terbaik keamanan yang direkomendasikan dan dipantau oleh Security Hub CSPM agar sesuai dengan persyaratan bisnis dan harapan keamanan Anda. Alih-alih menekan temuan untuk kontrol, Anda dapat menyesuaikan satu atau lebih parameternya untuk mendapatkan temuan yang sesuai dengan kebutuhan keamanan Anda.

Berikut adalah beberapa contoh kasus penggunaan untuk memodifikasi parameter kontrol dan menetapkan nilai kustom:

- [CloudWatch.16] — CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu

  Anda dapat menentukan periode waktu retensi.
- [IAM.7] — Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat

  Anda dapat menentukan parameter yang terkait dengan kekuatan kata sandi.
- [EC2.18] - Grup keamanan hanya boleh mengizinkan lalu lintas masuk yang tidak terbatas untuk port resmi

  Anda dapat menentukan port mana yang diizinkan untuk mengizinkan lalu lintas masuk yang tidak terbatas.
- [Lambda.5] - Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan

  Anda dapat menentukan jumlah minimum Zona Ketersediaan yang menghasilkan temuan yang diteruskan.

Bagian ini mencakup hal-hal yang perlu dipertimbangkan ketika Anda memodifikasi parameter kontrol.

Pengaruh memodifikasi nilai parameter kontrol

Saat Anda mengubah nilai parameter, Anda juga memicu pemeriksaan keamanan baru yang mengevaluasi kontrol berdasarkan nilai baru. Security Hub CSPM kemudian menghasilkan temuan kontrol baru berdasarkan nilai baru. Selama pembaruan berkala untuk mengontrol temuan, Security Hub CSPM juga menggunakan nilai parameter baru. Jika Anda mengubah nilai parameter untuk kontrol, tetapi belum mengaktifkan standar apa pun yang menyertakan kontrol, Security Hub CSPM tidak melakukan pemeriksaan keamanan apa pun menggunakan nilai baru. Anda harus mengaktifkan setidaknya satu standar yang relevan untuk Security Hub CSPM untuk mengevaluasi kontrol berdasarkan nilai parameter baru.

Kontrol dapat memiliki satu atau lebih parameter yang dapat disesuaikan. Jenis data yang mungkin untuk setiap parameter kontrol meliputi:

- Boolean
- Ganda
- Enum
- EnumList
- Bilangan Bulat
- IntegerList
- String
- StringList

Nilai parameter kustom berlaku di seluruh standar yang diaktifkan. Anda tidak dapat menyesuaikan parameter untuk kontrol yang tidak didukung di Wilayah Anda saat ini. Untuk daftar batas Regional untuk kontrol individual, lihatBatasan regional pada kontrol CSPM Security Hub.

Untuk beberapa kontrol, nilai parameter yang dapat diterima harus jatuh ke dalam rentang yang ditentukan agar valid. Dalam kasus ini, Security Hub CSPM menyediakan rentang yang dapat diterima.

Security Hub CSPM memilih nilai parameter default dan terkadang memperbaruinya. Setelah Anda menyesuaikan parameter kontrol, nilainya tetap menjadi nilai yang Anda tentukan untuk parameter kecuali Anda mengubahnya. Artinya, parameter berhenti melacak pembaruan ke nilai CSPM Hub Keamanan default, bahkan jika nilai kustom parameter cocok dengan nilai default saat ini yang ditentukan oleh Security Hub CSPM. Berikut contoh untuk kontrol [ACM.1] — Diimpor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu:

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
            }
        }
    }
```

```
}
```

Dalam contoh sebelumnya, `daysToExpiration` parameter memiliki nilai kustom`30`. Nilai default saat ini untuk parameter ini juga`30`. Jika Security Hub CSPM mengubah nilai default menjadi`14`, parameter dalam contoh ini tidak akan melacak perubahan itu. Ini akan mempertahankan nilai`30`.

Jika Anda ingin melacak pembaruan ke nilai CSPM Hub Keamanan default untuk parameter, setel `ValueType` bidang menjadi alih- `DEFAULT` alih. `CUSTOM` Untuk informasi selengkapnya, lihat Kembali ke parameter kontrol default dalam satu akun dan Wilayah.

Kontrol yang mendukung parameter khusus

Untuk daftar kontrol keamanan yang mendukung parameter kustom, lihat halaman Kontrol konsol CSPM Hub Keamanan atau. Referensi kontrol untuk Security Hub CSPM Untuk mengambil daftar ini secara terprogram, Anda dapat menggunakan operasi. ListSecurityControlDefinitions Dalam respons, `CustomizableProperties` objek menunjukkan kontrol mana yang mendukung parameter yang dapat disesuaikan.

Meninjau nilai parameter kontrol saat ini

Hal ini dapat membantu untuk mengetahui nilai parameter kontrol saat ini sebelum Anda memodifikasinya.

Anda dapat meninjau nilai saat ini untuk parameter kontrol individual di akun Anda. Jika Anda menggunakan konfigurasi pusat, administrator CSPM AWS Security Hub yang didelegasikan juga dapat meninjau nilai parameter yang ditentukan dalam kebijakan konfigurasi.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk meninjau nilai parameter kontrol saat ini.

Security Hub CSPM console

Untuk meninjau nilai parameter kontrol saat ini (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Kontrol. Pilih kontrol.
3. Pilih tab Parameter. Tab ini menunjukkan nilai parameter saat ini untuk kontrol.

Security Hub CSPM API

Untuk meninjau nilai parameter kontrol saat ini (API)

Memanggil BatchGetSecurityControls API, dan berikan satu atau lebih ID kontrol keamanan atau ARN. Ob `Parameters` jek dalam respons menunjukkan nilai parameter saat ini untuk kontrol yang ditentukan.

Misalnya, AWS CLI perintah berikut menunjukkan nilai parameter saat ini untuk`APIGatway.1`,`CloudWatch.15`, dan`IAM.7`. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Pilih metode pilihan Anda untuk melihat nilai parameter saat ini dalam kebijakan konfigurasi pusat.

Security Hub CSPM console

Untuk meninjau nilai parameter kontrol saat ini dalam kebijakan konfigurasi (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Masuk menggunakan kredensional akun administrator CSPM Security Hub yang didelegasikan di Wilayah beranda.
2. Di panel navigasi, pilih Peng aturan dan Konfigurasi.
3. Pada tab Kebijakan, pilih kebijakan konfigurasi, lalu pilih Lihat detail. Rincian kebijakan kemudian muncul, termasuk nilai parameter saat ini.

Security Hub CSPM API

Untuk meninjau nilai parameter kontrol saat ini dalam kebijakan konfigurasi (API)

1. Memanggil GetConfigurationPolicy API dari akun administrator yang didelegasikan di Wilayah beranda.
2. Berikan ARN atau ID kebijakan konfigurasi yang detailnya ingin Anda lihat. Respons mencakup nilai parameter saat ini.

Misalnya, AWS CLI perintah berikut mengambil nilai parameter kontrol saat ini dalam kebijakan konfigurasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Temuan kontrol juga mencakup nilai parameter kontrol saat ini. Di dalamnyaAWS Format Penemuan Keamanan (ASFF), nilai-nilai ini muncul di `Parameters` bidang `Compliance` objek. Untuk meninjau temuan di konsol CSPM Security Hub, pilih Temuan di panel navigasi. Untuk meninjau temuan secara terprogram, gunakan pen GetFindings goperasian Security Hub CSPM API.

Menyesuaikan nilai parameter kontrol

Petunjuk untuk menyesuaikan parameter kontrol bervariasi berdasarkan apakah Anda menggunakan konfigurasi pusat di AWS Security Hub CSPM. Konfigurasi pusat adalah fitur yang dapat digunakan administrator CSPM Hub Keamanan yang didelegasikan untuk mengonfigurasi kemampuan CSPM Security Hub di seluruh Wilayah AWS, akun, dan unit organisasi (OU).

Jika organisasi Anda menggunakan konfigurasi pusat, administrator yang didelegasikan dapat membuat kebijakan konfigurasi yang menyertakan parameter kontrol khusus. Kebijakan ini dapat dikaitkan dengan akun anggota dan OU yang dikelola secara terpusat, dan berlaku di Wilayah asal Anda dan semua Wilayah tertaut. Administrator yang didelegasikan juga dapat menetapkan satu atau lebih akun sebagai pengelola sendiri, yang memungkinkan pemilik akun untuk mengonfigurasi parameternya sendiri secara terpisah di setiap Wilayah. Jika organisasi Anda tidak menggunakan konfigurasi pusat, Anda harus menyesuaikan parameter kontrol secara terpisah di setiap akun dan Wilayah.

Sebaiknya gunakan konfigurasi pusat karena memungkinkan Anda menyelaraskan nilai parameter kontrol di berbagai bagian organisasi Anda. Misalnya, semua akun pengujian Anda mungkin menggunakan nilai parameter tertentu, dan semua akun produksi mungkin menggunakan nilai yang berbeda.

Menyesuaikan parameter kontrol di beberapa akun dan Wilayah

Jika Anda adalah administrator CSPM Hub Keamanan yang didelegasikan untuk organisasi yang menggunakan konfigurasi pusat, pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menyesuaikan parameter kontrol di beberapa akun dan Wilayah.

Security Hub CSPM console

Untuk menyesuaikan nilai parameter kontrol di beberapa akun dan Wilayah (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

   Pastikan Anda masuk ke Wilayah asal.
2. Di panel navigasi, pilih Peng aturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Untuk membuat kebijakan konfigurasi baru yang menyertakan parameter khusus, pilih Buat kebijakan. Untuk menentukan parameter kustom dalam kebijakan konfigurasi yang ada, pilih kebijakan, lalu pilih Edit.

   Untuk membuat kebijakan konfigurasi baru dengan nilai parameter kontrol khusus

   1. Di bagian Kebijakan khusus, pilih standar keamanan dan kontrol yang ingin Anda aktifkan.
   2. Pilih Sesuaikan parameter kontrol.
   3. Pilih kontrol, lalu tentukan nilai kustom untuk satu atau lebih parameter.
   4. Untuk menyesuaikan parameter untuk kontrol lainnya, pilih Ku stomisasi kontrol tambahan.
   5. Di bagian Akun, pilih akun atau OU yang ingin Anda terapkan kebijakan.
   6. Pilih Berikutnya.
   7. Pilih Buat kebijakan dan terapkan. Di Wilayah rumah Anda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun dan OU yang terkait dengan kebijakan konfigurasi ini. Akun dan OU dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari induk.

   Untuk menyesuaikan nilai parameter kontrol dalam kebijakan konfigurasi yang ada

1. Di bagian Kontrol, di bawah Kebijakan kustom, tentukan nilai parameter kustom baru yang Anda inginkan.
2. Jika ini adalah pertama kalinya Anda menyesuaikan parameter kontrol dalam kebijakan ini, pilih Ku stomisasi parameter kontrol, lalu pilih kontrol untuk disesuaikan. Untuk menyesuaikan parameter untuk kontrol lainnya, pilih Ku stomisasi kontrol tambahan.
3. Di bagian Akun, verifikasi akun atau OU yang ingin Anda terapkan kebijakan.
4. Pilih Berikutnya.
5. Tinjau perubahan Anda, dan verifikasi apakah mereka benar. Setelah selesai, pilih S impan kebijakan dan terapkan. Di Wilayah rumah Anda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun dan OU yang terkait dengan kebijakan konfigurasi ini. Akun dan OU dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari induk.

Security Hub CSPM API

Untuk menyesuaikan nilai parameter kontrol di beberapa akun dan Wilayah (API)

Untuk membuat kebijakan konfigurasi baru dengan nilai parameter kontrol khusus

1. Memanggil CreateConfigurationPolicy API dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `SecurityControlCustomParameters` objek, berikan pengenal setiap kontrol yang ingin Anda sesuaikan.
3. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, sedi `CUSTOM` akan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. Bid `Value` ang tidak boleh kosong saat `ValueType` berada`CUSTOM`. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan memanggil GetSecurityControlDefinition API.

Untuk menyesuaikan nilai parameter kontrol dalam kebijakan konfigurasi yang ada

1. Memanggil UpdateConfigurationPolicy API dari akun administrator yang didelegasikan di Wilayah beranda.

2. Untuk `Identifier` bidang tersebut, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan konfigurasi yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengenal setiap kontrol yang ingin Anda sesuaikan.
4. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, sedi `CUSTOM` akan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan memanggil GetSecurityControlDefinition API.

Misalnya, AWS CLI perintah berikut membuat kebijakan konfigurasi baru dengan nilai kustom untuk `daysToExpiration` parameter`ACM.1`. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}}]}}}'
```

Menyesuaikan parameter kontrol dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda dapat menyesuaikan parameter kontrol untuk akun Anda di satu Wilayah pada satu waktu saja.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menyesuaikan parameter kontrol. Perubahan Anda hanya berlaku untuk akun Anda di Wilayah saat ini. Untuk menyesuaikan parameter kontrol di Wilayah tambahan, ulangi langkah-langkah berikut di setiap akun tambahan dan Wilayah tempat Anda ingin menyesuaikan parameter. Kontrol yang sama dapat menggunakan nilai parameter yang berbeda di Wilayah yang berbeda.

Security Hub CSPM console

Untuk menyesuaikan nilai parameter kontrol dalam satu akun dan Wilayah (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Kontrol. Dalam tabel, pilih kontrol yang mendukung parameter kustom dan Anda ingin mengubah parameternya. Kol om parameter kustom menunjukkan kontrol mana yang mendukung parameter kustom.
3. Pada halaman detail untuk kontrol, pilih tab Parameter, lalu pilih Edit.
4. Tentukan nilai parameter yang Anda inginkan.
5. Secara opsional, di bagian Alasan perubahan, pilih alasan untuk menyesuaikan parameter.
6. Pilih Simpan.

Security Hub CSPM API

Untuk menyesuaikan nilai parameter kontrol dalam satu akun dan Wilayah (API)

1. Memanggil UpdateSecurityControl API.
2. Untuk`SecurityControlId`, berikan ID kontrol yang ingin Anda sesuaikan.
3. Untuk `Parameters` objek, berikan nama setiap parameter yang ingin Anda sesuaikan. Untuk setiap parameter yang Anda sesuaikan, sedi `CUSTOM` akan`ValueType`. Untuk`Value`, berikan tipe data parameter dan nilai kustom. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilainya saat ini. Anda dapat menemukan parameter yang didukung, tipe data, dan nilai yang valid untuk kontrol dengan memanggil GetSecurityControlDefinition API.
4. Secara opsional`LastUpdateReason`, untuk, berikan alasan untuk menyesuaikan parameter kontrol.

Misalnya, AWS CLI perintah berikut mendefinisikan nilai kustom untuk `daysToExpiration` parameter`ACM.1`. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
```

```
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer":
 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Mengembalikan ke nilai parameter kontrol default

Parameter kontrol dapat memiliki nilai default yang ditetapkan oleh AWS Security Hub CSPM. Kadang-kadang, Security Hub CSPM memperbarui nilai default untuk parameter untuk mencerminkan praktik terbaik keamanan yang berkembang. Jika Anda belum menentukan nilai kustom untuk parameter kontrol, kontrol secara otomatis melacak pembaruan tersebut dan menggunakan nilai default baru.

Anda dapat kembali menggunakan nilai parameter default untuk kontrol. Petunjuk untuk pengembalian tergantung pada apakah Anda menggunakan konfigurasi pusat di Security Hub CSPM. Konfigurasi pusat adalah fitur yang dapat digunakan administrator CSPM Hub Keamanan yang didelegasikan untuk mengonfigurasi kemampuan CSPM Security Hub di seluruh Wilayah AWS, akun, dan unit organisasi (OU).

> **Note**
>
> Tidak semua parameter kontrol memiliki nilai CSPM Hub Keamanan default. Dalam kasus seperti itu, ketika `ValueType` disetel ke`DEFAULT`, tidak ada nilai default spesifik yang digunakan CSPM Security Hub. Sebaliknya, Security Hub CSPM mengabaikan parameter tanpa adanya nilai kustom.

Kembali ke parameter kontrol default di beberapa akun dan Wilayah

Jika Anda menggunakan konfigurasi pusat, Anda dapat mengembalikan parameter kontrol untuk beberapa akun dan OU yang dikelola secara terpusat di Wilayah rumah dan Wilayah tertaut.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk kembali ke nilai parameter default di beberapa akun dan Wilayah menggunakan konfigurasi pusat.

Security Hub CSPM console

Untuk kembali ke nilai parameter kontrol default di beberapa akun dan Wilayah (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/

Masuk menggunakan kredensional akun administrator CSPM Security Hub yang didelegasikan di Wilayah beranda.

2. Di panel navigasi, pilih Peng aturan dan Konfigurasi.
3. Pilih tab Kebijakan.
4. Pilih kebijakan, lalu pilih Edit.
5. Di bawah Kebijakan kustom, bagian Kontrol menampilkan daftar kontrol yang Anda tentukan parameter kustom.
6. Temukan kontrol yang memiliki satu atau lebih nilai parameter untuk dikembalikan. Kemudian, pilih Hapus untuk kembali ke nilai default.
7. Di bagian Akun, verifikasi akun atau OU yang ingin Anda terapkan kebijakan.
8. Pilih Berikutnya.
9. Tinjau perubahan Anda, dan verifikasi apakah mereka benar. Setelah selesai, pilih S impan kebijakan dan terapkan. Di Wilayah rumah Anda dan semua Wilayah yang ditautkan, tindakan ini mengesampingkan pengaturan konfigurasi akun dan OU yang terkait dengan kebijakan konfigurasi ini. Akun dan OU dapat dikaitkan dengan kebijakan konfigurasi melalui aplikasi langsung atau warisan dari induk.

Security Hub CSPM API

Untuk kembali ke nilai parameter kontrol default di beberapa akun dan Wilayah (API)

1. Memanggil UpdateConfigurationPolicy API dari akun administrator yang didelegasikan di Wilayah beranda.
2. Untuk `Identifier` bidang tersebut, berikan Nama Sumber Daya Amazon (ARN) atau ID kebijakan yang ingin Anda perbarui.
3. Untuk `SecurityControlCustomParameters` objek, berikan pengenal setiap kontrol yang ingin Anda kembalikan satu atau lebih parameter.
4. Di `Parameters` objek, untuk setiap parameter yang ingin Anda kembalikan, berikan `DEFAULT` untuk `ValueType` bidang. Bila `ValueType` diset `DEFAULT` el ke, Anda tidak perlu memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub CSPM mengabaikannya. Jika permintaan Anda menghilangkan parameter yang didukung kontrol, parameter tersebut mempertahankan nilai saat ini.

> **Warning**
>
> Jika Anda menghilangkan objek kontrol dari `SecurityControlCustomParameters` bidang, Security Hub CSPM mengembalikan semua parameter kustom untuk kontrol ke nilai defaultnya. Daftar yang benar-benar kosong untuk `SecurityControlCustomParameters` mengembalikan parameter khusus untuk semua kontrol ke nilai defaultnya.

Misalnya, AWS CLI perintah berikut mengembalikan parameter `daysToExpiration` kontrol untuk `ACM.1` ke nilai defaultnya dalam kebijakan konfigurasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--name "TestConfigurationPolicy" \
--description "Updated configuration policy" \
--updated-reason "Revert ACM.1 parameter to default value"
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
 "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
 "SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
 {"daysToExpiration": {"ValueType": "DEFAULT"}}}]}}}'
```

Kembali ke parameter kontrol default dalam satu akun dan Wilayah

Jika Anda tidak menggunakan konfigurasi pusat atau memiliki akun yang dikelola sendiri, Anda dapat kembali menggunakan nilai parameter default untuk akun Anda di satu Wilayah pada satu waktu.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk kembali ke nilai parameter default untuk akun Anda di satu Wilayah. Untuk kembali ke nilai parameter default di Wilayah tambahan, ulangi langkah-langkah ini di setiap Wilayah tambahan.

> **Note**
>
> Jika Anda menonaktifkan Security Hub CSPM, parameter kontrol kustom Anda diatur ulang. Jika Anda mengaktifkan Security Hub CSPM lagi di masa mendatang, semua kontrol akan menggunakan nilai parameter default untuk memulai.

Security Hub CSPM console

Untuk kembali ke nilai parameter kontrol default dalam satu akun dan Wilayah (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Kontrol. Pilih kontrol yang ingin Anda kembalikan ke nilai parameter default.
3. Pada `Parameters` tab, pilih Dis esuaikan di sebelah parameter kontrol. Kemudian, pilih H apus kustomisasi. Parameter ini sekarang menggunakan nilai CSPM Hub Keamanan default dan melacak pembaruan mendatang ke nilai default.
4. Ulangi langkah sebelumnya untuk setiap nilai parameter yang ingin Anda kembalikan.

Security Hub CSPM API

Untuk kembali ke nilai parameter kontrol default dalam satu akun dan Wilayah (API)

1. Memanggil UpdateSecurityControl API.
2. Untuk`SecurityControlId`, berikan ARN atau ID kontrol yang parameternya ingin Anda kembalikan.
3. Di `Parameters` objek, untuk setiap parameter yang ingin Anda kembalikan, berikan `DEFAULT` untuk `ValueType` bidang. Bila `ValueType` diset `DEFAULT` el ke, Anda tidak perlu memberikan nilai untuk `Value` bidang tersebut. Jika nilai disertakan dalam permintaan Anda, Security Hub CSPM mengabaikannya.
4. Secara opsional`LastUpdateReason`, for, berikan alasan untuk kembali ke nilai parameter default.

Misalnya, AWS CLI perintah berikut mengembalikan parameter `daysToExpiration` kontrol untuk `ACM.1` ke nilai defaultnya. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
--last-update-reason "New internal requirement"
```

Memeriksa status perubahan parameter kontrol

Saat Anda mencoba menyesuaikan parameter kontrol atau kembali ke nilai default, Anda dapat memvalidasi apakah perubahan yang diinginkan efektif. Ini membantu memastikan bahwa kontrol berfungsi seperti yang Anda harapkan dan memberikan nilai keamanan yang diinginkan. Jika pembaruan parameter tidak berhasil, Security Hub CSPM mempertahankan nilai parameter saat ini.

Untuk memverifikasi bahwa pembaruan parameter berhasil, Anda dapat meninjau detail kontrol pada konsol CSPM Hub Keamanan. Di konsol, pilih Kontrol pada panel navigasi. Kemudian, pilih kontrol untuk menampilkan detailnya. Tab Parameter menunjukkan status perubahan parameter.

Secara terprogram, jika permintaan Anda untuk memperbarui parameter valid, nilai `UpdateStatus` bidang tersebut merupakan `UPDATING` respons terhadap operasi. BatchGetSecurityControls Ini berarti pembaruan valid, tetapi semua temuan mungkin belum menyertakan nilai parameter yang diperbarui. Ketika nilai `UpdateState` berubah menjadi`READY`, Security Hub CSPM menggunakan nilai parameter kontrol yang diperbarui saat menjalankan pemeriksaan keamanan kontrol. Temuan termasuk nilai parameter yang diperbarui.

`UpdateSecurityControl`Operasi mengembalikan `InvalidInputException` respons untuk nilai parameter yang tidak valid. Tanggapan memberikan rincian tambahan tentang alasan kegagalan. Misalnya, Anda mungkin telah menentukan nilai yang berada di luar rentang yang valid untuk parameter. Atau, Anda mungkin telah menentukan nilai yang tidak menggunakan tipe data yang benar. Kirim permintaan Anda lagi dengan masukan yang valid.

Jika kegagalan internal terjadi saat Anda mencoba memperbarui nilai parameter, Security Hub CSPM akan mencoba lagi secara otomatis jika Anda telah mengaktifkan. AWS Config Lihat informasi yang lebih lengkap di Pertimbangan sebelum mengaktifkan dan mengonfigurasi AWS Config.

Meninjau dan mengelola temuan kontrol di Security Hub CSPM

Halaman detail kontrol menampilkan daftar temuan aktif untuk kontrol. Daftar ini tidak termasuk temuan yang diarsipkan.

Halaman detail kontrol mendukung agregasi lintas wilayah. Jika Anda telah menetapkan Wilayah agregasi, status kontrol dan daftar pemeriksaan keamanan pada halaman detail kontrol mencakup pemeriksaan dari semua yang ditautkanWilayah AWS.

Daftar ini menyediakan alat untuk memfilter dan mengurutkan temuan, sehingga Anda dapat fokus pada temuan yang lebih mendesak terlebih dahulu. Temuan dapat mencakup tautan ke detail sumber daya di konsol layanan terkait. Untuk kontrol yang didasarkan pada AWS Config aturan, Anda dapat melihat detail tentang aturan.

Anda juga dapat menggunakan AWS Security Hub CSPM API untuk mengambil daftar temuan dan menemukan detail.

Untuk informasi selengkapnya, lihat Meninjau detail dan sejarah temuan.

Untuk mencerminkan status investigasi Anda saat ini atas temuan kontrol, Anda menetapkan status alur kerja. Untuk informasi selengkapnya, lihat the section called “Mengatur status alur kerja temuan”.

Anda juga dapat mengirim temuan CSPM Security Hub yang dipilih ke tindakan kustom di Amazon. EventBridge Untuk informasi selengkapnya, lihat the section called “Mengirim temuan ke tindakan khusus”.

Topik

- Penyaringan dan penyortiran temuan kontrol
- Sampel temuan kontrol

Penyaringan dan penyortiran temuan kontrol

Memilih kontrol dari halaman Kontrol konsol CSPM AWS Security Hub atau dari halaman detail standar akan membawa Anda ke halaman detail kontrol.

Halaman detail kontrol menunjukkan judul dan deskripsi kontrol, status kontrol keseluruhan, dan rincian pemeriksaan keamanan untuk kontrol dalam 24 jam terakhir.

Gunakan opsi Filter menurut di samping daftar pemeriksaan kontrol untuk dengan cepat fokus pada temuan dengan status alur kerja atau status kepatuhan tertentu.

Selain opsi Filter menurut, Anda dapat menggunakan kotak Tambahkan filter untuk memfilter daftar centang menurut bidang lain, seperti Akun AWS ID atau ID sumber daya.

Secara default, temuan dengan status kepatuhan LULUS dicantumkan terlebih dahulu. Anda dapat mengubah penyortiran default dengan memilih opsi yang berbeda di header kolom.

Dari halaman detail kontrol, Anda dapat memilih Unduh untuk mengunduh halaman temuan kontrol saat ini ke file.csv.

Jika Anda memfilter daftar temuan, maka unduhan hanya menyertakan kontrol yang cocok dengan filter. Jika Anda memilih temuan spesifik dari daftar, maka unduhan hanya menyertakan temuan yang dipilih.

Untuk informasi lebih lanjut tentang temuan penyaringan, lihatPenyaringan temuan di Security Hub CSPM.

Sampel temuan kontrol

Sampel berikut memberikan contoh temuan kontrol CSPM AWS Security Hub dalam AWS Security Finding Format (ASFF). Isi temuan kontrol bervariasi tergantung pada apakah Anda mengaktifkan temuan kontrol konsolidasi.

Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Security Hub CSPM menghasilkan satu temuan untuk kontrol, bahkan jika kontrol tersebut berlaku untuk beberapa standar yang diaktifkan. Jika Anda tidak mengaktifkan fitur ini, Security Hub CSPM akan menghasilkan temuan kontrol terpisah untuk setiap standar yang diaktifkan yang diterapkan kontrol. Misalnya, jika Anda mengaktifkan dua standar dan kontrol berlaku untuk keduanya, Anda menerima dua temuan terpisah untuk kontrol, satu untuk setiap standar. Jika Anda mengaktifkan temuan kontrol terkonsolidasi, Anda hanya menerima satu temuan untuk kontrol. Untuk informasi selengkapnya, lihat Temuan kontrol konsolidasi.

Sampel di halaman ini memberikan contoh untuk kedua skenario. Sampel meliputi: temuan kontrol untuk standar CSPM Security Hub individu ketika temuan kontrol konsolidasi dinonaktifkan, dan temuan kontrol untuk beberapa standar CSPM Security Hub ketika temuan kontrol konsolidasi diaktifkan.

Sampel temuan kontrol

- Temuan sampel untukAWSStandar Praktik Terbaik Keamanan Dasar
- Temuan sampel untuk CISAWSTolok Ukur Yayasan v5.0.0
- Temuan sampel untuk CISAWSTolok Ukur Yayasan v3.0.0
- Temuan sampel untuk CISAWSTolok Ukur Yayasan v1.4.0
- Temuan sampel untuk CISAWSTolok Ukur Yayasan v1.2.0
- Temuan sampel untuk standar NIST SP 800-53 Revisi 5
- Temuan sampel untuk standar NIST SP 800-171 Revisi 2

- Temuan sampel untuk Standar Keamanan Data Industri Kartu Pembayaran v3.2.1
- Temuan sampel untukAWSStandar Penandaan Sumber Daya
- Temuan sampel untukAWS Control Towerstandar yang dikelola layanan
- Sampel temuan konsolidasi untuk beberapa standar

> **Note**
>
> Temuan kontrol mengacu pada berbagai bidang dan nilai di Wilayah dan AWS GovCloud (US) Wilayah Tiongkok. Untuk informasi selengkapnya, lihat Dampak konsolidasi pada bidang dan nilai ASFF.

Temuan sampel untukAWSStandar Praktik Terbaik Keamanan Dasar

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar Praktik Terbaik Keamanan AWS Dasar (FSBP). Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
```

```
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
```

```
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
    ]
  }
}
```

Temuan sampel untuk CISAWSTolok Ukur Yayasan v5.0.0

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk CIS AWS Foundations Benchmark v5.0.0. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "AwsAccountId": "123456789012",
  "CompanyName": "AWS",
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.7",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v5.0.0/5.1.1"
    ],
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/5.0.0"
      }
    ]
```

```
  },
  "CreatedAt": "2025-10-10T17:04:00.952Z",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
 Foundations Benchmark"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Product": 40,
      "Original": "MEDIUM"
    }
  },
  "FirstObservedAt": "2025-10-10T17:03:57.895Z",
  "GeneratorId": "cis-aws-foundations-benchmark/v/5.0.0/5.1.1",
  "Id": "arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
  "LastObservedAt": "2025-10-14T05:22:28.667Z",
  "ProcessedAt": "2025-10-14T05:22:50.099Z",
  "ProductArn": "arn:aws:securityhub:us-west-1::product/aws/securityhub",
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
west-1:123456789012:subscription/cis-aws-foundations-benchmark/v/5.0.0",
    "ControlId": "5.1.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2a99554f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-west-1:123456789012:control/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-1::product/aws/
securityhub/arn:aws:securityhub:us-west-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/5.0.0/5.1.1/finding/443a9d3f-8a59-4fa0-8e2c-EXAMPLE111",
    "PreviousComplianceStatus": "FAILED"
```

```
  },
  "ProductName": "Security Hub CSPM",
  "RecordState": "ACTIVE",
  "Region": "us-west-1",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
 Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "Resources": [
    {
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-west-1",
      "Type": "AwsAccount"
    }
  ],
  "SchemaVersion": "2018-10-08",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM",
    "Product": 40
  },
  "Title": "5.1.1 EBS default encryption should be enabled",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "UpdatedAt": "2025-10-14T05:22:38.671Z",
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW"
}
```


Temuan sampel untuk CISAWSTolok Ukur Yayasan v3.0.0

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk CIS AWS Foundations Benchmark v3.0.0. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
 the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
 at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/
remediation",
```

```
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
```

```
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  },
  "ProcessedAt": "2024-04-23T07:47:07.088Z"
}
```

Temuan sampel untuk CISAWSTolok Ukur Yayasan v1.4.0

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk CIS AWS Foundations Benchmark v1.4.0. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS CloudTrailis a web service that recordsAWSAPI calls for an
 account and makes those logs available to users and resources in accordance with IAM
 policies.AWS Key Management Service(KMS) is a managed service that helps create and
 control the encryption keys used to encrypt account data, and uses Hardware Security
 Modules (HSMs) to protect the security of encryption keys. CloudTrail logs can be
 configured to leverage server side encryption (SSE) andAWS KMScustomer created master
```

```
 keys (CMK) to further protect CloudTrail logs. It is recommended that CloudTrail be
 configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/cis-aws-foundations-benchmark/
v/1.4.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
    "ControlId": "3.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CISAWSFoundations Benchmark v1.4.0/3.7"
    ],
```

```
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  }
}
```

Temuan sampel untuk CISAWSTolok Ukur Yayasan v1.2.0

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk CIS AWS Foundations Benchmark v1.2.0. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
  ],
  "FirstObservedAt": "2020-08-29T04:10:06.337Z",
```

```
  "LastObservedAt": "2021-09-28T16:10:05.350Z",
  "CreatedAt": "2020-08-29T04:10:06.337Z",
  "UpdatedAt": "2021-09-28T16:10:00.087Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
  "Description": "AWS Key Management Service(KMS) is a managed service that helps
 create and control the encryption keys used to encrypt account data, and uses Hardware
 Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
 logs can be configured to leverage server side encryption (SSE) and KMS customer
 created master keys (CMK) to further protect CloudTrail logs. It is recommended that
 CloudTrail be configured to use SSE-KMS.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
    "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
    "RuleId": "2.7",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
```

```
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/
CISAWSFoundations Benchmark"
    ]
  }
}
```

Temuan sampel untuk standar NIST SP 800-53 Revisi 5

Sampel berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar NIST SP 800-53 Revisi 5. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
```

```
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2023-02-17T14:22:46.726Z",
  "LastObservedAt": "2023-02-17T14:22:50.846Z",
  "CreatedAt": "2023-02-17T14:22:46.726Z",
  "UpdatedAt": "2023-02-17T14:22:46.726Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to fix this issue, consult theAWSSecurity Hub CSPM
 NIST 800-53 R5 documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-53/v/5.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-53/v/5.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
```

```
    "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/
v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",

      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",

      "Partition": "aws",

      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
        "NIST.800-53.r5 AU-9",
        "NIST.800-53.r5 CA-9(1)",
        "NIST.800-53.r5 CM-3(6)",
        "NIST.800-53.r5 SC-13",
        "NIST.800-53.r5 SC-28",
        "NIST.800-53.r5 SC-28(1)",
        "NIST.800-53.r5 SC-7(10)",
        "NIST.800-53.r5 SI-7(6)"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/nist-800-53/v/5.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
```

```
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2023-02-17T14:22:53.572Z"
}
```

Temuan sampel untuk standar NIST SP 800-171 Revisi 2

Sampel berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar NIST SP 800-171 Revisi 2. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/v/2.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "nist-800-171/v/2.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "AwsAccountName": "TestAcct",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2025-05-29T05:23:58.690Z",
  "LastObservedAt": "2025-05-30T05:50:11.898Z",
  "CreatedAt": "2025-05-29T05:24:24.772Z",
  "UpdatedAt": "2025-05-30T05:50:34.292Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
```

```
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/nist-800-171/v/2.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/nist-800-171/v/2.0.0",
    "ControlId": "CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-0ab1c2d4",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/
nist-800-171/v/2.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-171/
v/2.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Id": "arn:aws:cloudtrail:ca-central-1:123456789012:trail/aws-
BaselineCloudTrail",
      "Partition": "aws",
      "Region": "us-east-1",
      "Type": "AwsCloudTrailTrail"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "NIST.800-171.r2/3.3.8"
    ],
    "AssociatedStandards": [
      {
```

```
        "StandardsId": "standards/nist-800-171/v/2.0.0"
      }
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Product": 40,
      "Label": "MEDIUM",
      "Normalized": 40,
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T05:50:40.297Z"
}
```

Temuan sampel untuk Standar Keamanan Data Industri Kartu Pembayaran v3.2.1

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk Payment Card Industry Data Security Standard (PCI DSS) v3.2.1. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
```

```
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest usingAWS
 KMSCMKs",
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/pci-dss/v/3.2.1",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
    "ControlId": "PCI.CloudTrail.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
```

```
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "PCI DSS 3.4"
    ],
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/pci-dss/v/3.2.1"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
    ]
  }
}
```

Temuan sampel untukAWSStandar Penandaan Sumber Daya

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar AWS Resource Tagging. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
```

```
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the
 specific keys defined in the parameter requiredTagKeys. The control fails if the
 subnet doesn't have any tag keys or if it doesn't have all the keys specified in
 the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
 control only checks for the existence of a tag key and fails if the subnet isn't
 tagged with any key. System tags, which are automatically applied and begin with aws:,
 are ignored.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "No tags are present.",
    "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
    "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
```

```
    {
      "Type": "AwsEc2Subnet",
      "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
      "Partition": "aws",
      "Region": "eu-central-1",
      "Details": {
        "AwsEc2Subnet": {
          "AssignIpv6AddressOnCreation": false,
          "AvailabilityZone": "eu-central-1b",
          "AvailabilityZoneId": "euc1-az3",
          "AvailableIpAddressCount": 4091,
          "CidrBlock": "10.24.34.0/23",
          "DefaultForAz": true,
          "MapPublicIpOnLaunch": true,
          "OwnerId": "123456789012",
          "State": "available",
          "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
          "SubnetId": "subnet-1234567890abcdef0",
          "VpcId": "vpc-021345abcdef6789"
        }
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ],
            },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
```

```
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Temuan sampel untukAWS Control Towerstandar yang dikelola layanan

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk standar yang AWS Control Tower dikelola layanan. Dalam sampel ini, temuan kontrol konsolidasi dinonaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-
control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub CSPM",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
```

```
  "Description": "ThisAWScontrol checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub:::standards/service-managed-aws-control-tower/
v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
    "ControlId": "CT.CloudTrail.2",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-
managed-aws-control-tower/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub CSPM",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-
aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS::::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
```

```
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  }
}
```

Sampel temuan konsolidasi untuk beberapa standar

Contoh berikut memberikan contoh temuan untuk kontrol yang berlaku untuk beberapa standar yang diaktifkan. Dalam sampel ini, temuan kontrol terkonsolidasi diaktifkan.

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-08-09T14:57:04.521Z",
  "LastObservedAt": "2025-05-30T03:30:17.407Z",
  "CreatedAt": "2024-08-09T14:57:04.521Z",
  "UpdatedAt": "2025-05-30T03:30:32.781Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40,
```

```
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whetherAWS CloudTrailis configured to use the
 server side encryption (SSE)AWS Key Management Service(AWS KMS) customer master key
 (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult theAWSSecurity Hub
 CSPM controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-01a2b345",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-
NOT-DELETE",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/TestTrail-DO-NOT-DELETE",
      "Partition": "aws",
      "Region": "us-east-1",
      "Details": {
        "AwsCloudTrailTrail": {
          "HasCustomEventSelectors": false,
          "IncludeGlobalServiceEvents": true,
          "LogFileValidationEnabled": true,
          "HomeRegion": "us-east-1",
          "IsMultiRegionTrail": true,
          "S3BucketName": "cloudtrail-awslogs-do-not-delete",
          "IsOrganizationTrail": false,
          "Name": "TestTrail-DO-NOT-DELETE"
        }
      }
    }
```

```
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v1.2.0/2.7",
      "CIS AWS Foundations Benchmark v1.4.0/3.7",
      "CIS AWS Foundations Benchmark v3.0.0/3.5",
      "NIST.800-171.r2/3.3.8",
      "PCI DSS v3.2.1/3.4",
      "PCI DSS v4.0.1/10.3.2"
    ],
    "AssociatedStandards": [
      { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
      { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
      { "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"},
      { "StandardsId": "standards/nist-800-171/v/2.0.0"},
      { "StandardsId": "standards/pci-dss/v/3.2.1"},
      { "StandardsId": "standards/pci-dss/v/4.0.1"}
    ]
  },
  "Workflow": {
    "Status": "NEW"
  },
  "WorkflowState": "NEW",
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ],
    "Severity": {
      "Normalized": 40,
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "ProcessedAt": "2025-05-30T03:31:00.831Z"
}
```

Memahami integrasi di Security Hub CSPM

AWS Security Hub CSPM dapat menyerap temuan keamanan dari beberapa solusi keamanan pihak ketiga Layanan AWS AWS Partner Network yang didukung. Integrasi ini dapat membantu Anda mendapatkan pandangan komprehensif tentang keamanan dan kepatuhan di seluruh AWS lingkungan Anda. Security Hub CSPM menyerap temuan dari solusi terintegrasi dan mengubahnya menjadi AWS Security Finding Format (ASFF).

> **Important**
>
> Untuk integrasi produk yang didukung AWS dan pihak ketiga, Security Hub CSPM menerima dan mengkonsolidasikan temuan yang dihasilkan hanya setelah Anda mengaktifkan Security Hub CSPM untuk Anda. Akun AWS Layanan tidak menerima dan mengkonsolidasikan temuan keamanan yang dihasilkan sebelum Anda mengaktifkan Security Hub CSPM.

Halaman Integrasi konsol CSPM Security Hub menyediakan akses ke integrasi produk yang tersedia AWS dan pihak ketiga. Security Hub CSPM API juga memiliki operasi untuk mengelola integrasi.

Integrasi mungkin tidak tersedia di semua Wilayah AWS. Jika integrasi tidak didukung di Wilayah tempat Anda saat ini masuk di konsol CSPM Hub Keamanan, integrasi tersebut tidak muncul di halaman Integrasi konsol. Untuk daftar integrasi yang tersedia di Wilayah China dan AWS GovCloud (US) Regions, lihatKetersediaan integrasi menurut Wilayah.

Selain integrasi pihak ketiga bawaan, Anda dapat mengintegrasikan produk keamanan khusus dengan Security Hub CSPM. Layanan AWS Anda kemudian dapat mengirim temuan dari produk ini ke Security Hub CSPM dengan menggunakan Security Hub CSPM API. Anda juga dapat menggunakan API untuk memperbarui temuan yang ada yang diterima Security Hub CSPM dari produk keamanan khusus.

Topik

- Meninjau daftar integrasi CSPM Security Hub
- Mengaktifkan aliran temuan dari integrasi CSPM Security Hub
- Menonaktifkan aliran temuan dari integrasi CSPM Security Hub
- Melihat temuan dari integrasi CSPM Security Hub
- Layanan AWS integrasi dengan Security Hub CSPM
- Third-party integrasi produk dengan Security Hub CSPM

- Mengintegrasikan Security Hub CSPM dengan produk khusus

Meninjau daftar integrasi CSPM Security Hub

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk meninjau daftar integrasi di AWS Security Hub CSPM atau detail tentang integrasi tertentu.

Security Hub CSPM console

Untuk meninjau opsi dan detail integrasi (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi CSPM Hub Keamanan, pilih Integrasi.

Pada halaman Integrasi, integrasi dengan yang lain dicantumkan Layanan AWS terlebih dahulu, diikuti dengan integrasi dengan produk pihak ketiga.

Untuk setiap integrasi, halaman Integrasi menyediakan informasi berikut:

- Nama perusahaan
- Nama produk
- Deskripsi integrasi
- Kategori yang diterapkan integrasi
- Cara mengaktifkan integrasi
- Status integrasi saat ini

Anda dapat memfilter daftar dengan memasukkan teks dari bidang berikut:

- Nama perusahaan
- Nama produk
- Deskripsi integrasi
- Kategori

Security Hub CSPM API

Untuk meninjau opsi dan detail integrasi (API)

Untuk mendapatkan daftar integrasi, gunakan DescribeProducts operasi. Jika Anda menggunakan AWS CLI, jalankan describe-products perintah.

Untuk mengambil detail untuk integrasi produk tertentu, gunakan `ProductArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari integrasi.

Misalnya, AWS CLI perintah berikut mengambil detail tentang integrasi Security Hub CSPM dengan 3CoreSec.

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Mengaktifkan aliran temuan dari integrasi CSPM Security Hub

Pada halaman Integrasi konsol CSPM AWS Security Hub, Anda dapat melihat langkah-langkah yang diperlukan untuk mengaktifkan setiap integrasi.

Untuk sebagian besar integrasi dengan yang lain Layanan AWS, satu-satunya langkah yang diperlukan untuk mengaktifkan integrasi adalah mengaktifkan layanan lain. Informasi integrasi termasuk tautan ke halaman beranda layanan lain. Saat Anda mengaktifkan layanan lain, izin tingkat sumber daya yang memungkinkan Security Hub CSPM menerima temuan dari layanan kemudian secara otomatis dibuat dan diterapkan.

Untuk integrasi produk pihak ketiga, Anda mungkin perlu membeli integrasi dari AWS Marketplace, dan kemudian mengkonfigurasi integrasi. Informasi integrasi menyediakan tautan untuk menyelesaikan tugas-tugas ini.

Jika tersedia lebih dari satu versi produk AWS Marketplace, pilih versi yang ingin Anda berlangganan, lalu pilih L anjutkan untuk Berlangganan. Misalnya, beberapa produk menawarkan versi standar dan AWS GovCloud (US) versi.

Saat Anda mengaktifkan integrasi produk, kebijakan sumber daya secara otomatis dilampirkan ke langganan produk tersebut. Kebijakan sumber daya ini menentukan izin yang dibutuhkan CSPM Security Hub untuk menerima temuan dari produk tersebut.

Setelah Anda menyelesaikan langkah awal untuk mengaktifkan integrasi, Anda kemudian dapat menonaktifkan dan mengaktifkan kembali aliran temuan dari integrasi tersebut. Pada halaman Integrasi, untuk integrasi yang mengirimkan temuan, informasi Status menunjukkan apakah Anda saat ini menerima temuan.

Security Hub CSPM console

Untuk mengaktifkan aliran temuan dari integrasi (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi CSPM Hub Keamanan, pilih Integrasi.
3. Untuk integrasi yang mengirimkan temuan, informasi Status menunjukkan apakah Security Hub CSPM saat ini menerima temuan dari integrasi tersebut.
4. Pilih Terima temuan.

Security Hub CSPM API

Gunakan EnableImportFindingsForProduct operasi. Jika Anda menggunakan AWS CLI, jalankan enable-import-findings-for-product perintah. Untuk mengaktifkan Security Hub untuk menerima temuan dari integrasi, Anda memerlukan produk ARN. Untuk mendapatkan ARN untuk integrasi yang tersedia, gunakan operasi. DescribeProducts Jika Anda menggunakan AWS CLI, jalankan describe-products.

Misalnya, AWS CLI perintah berikut memungkinkan Security Hub CSPM untuk menerima temuan dari integrasi CrowdStrike Falcon. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Menonaktifkan aliran temuan dari integrasi CSPM Security Hub

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menonaktifkan aliran temuan dari integrasi AWS Security Hub CSPM.

Security Hub CSPM console

Untuk menonaktifkan aliran temuan dari integrasi (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi CSPM Hub Keamanan, pilih Integrasi.
3. Untuk integrasi yang mengirimkan temuan, informasi Status menunjukkan apakah Security Hub CSPM saat ini menerima temuan dari integrasi tersebut.

4. Pilih Ber henti menerima temuan.

Security Hub CSPM API

Gunakan DisableImportFindingsForProduct operasi. Jika Anda menggunakan AWS CLI, jalankan disable-import-findings-for-product perintah. Untuk menonaktifkan aliran temuan dari integrasi, Anda memerlukan ARN berlangganan untuk integrasi yang diaktifkan. Untuk mendapatkan langganan ARN, gunakan ListEnabledProductsForImport operasi. Jika Anda menggunakan AWS CLI, jalankan list-enabled-products-for-import.

Misalnya, AWS CLI perintah berikut menonaktifkan aliran temuan ke Security Hub CSPM dari integrasi Falcon CrowdStrike . Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

Melihat temuan dari integrasi CSPM Security Hub

Saat Anda mulai menerima temuan dari integrasi CSPM Hub AWS Keamanan, halaman Integrasi konsol CSPM Hub Keamanan menampilkan Status integrasi sebagai Menerima temuan. Untuk meninjau daftar temuan dari integrasi, pilih Lihat temuan.

Daftar temuan menunjukkan temuan aktif untuk integrasi yang dipilih yang memiliki status alur kerja `NEW` atau`NOTIFIED`.

Jika Anda mengaktifkan agregasi lintas wilayah, maka di Wilayah agregasi, daftar mencakup temuan dari Wilayah agregasi dan dari Wilayah tertaut tempat integrasi diaktifkan. Security Hub tidak secara otomatis mengaktifkan integrasi berdasarkan konfigurasi agregasi lintas wilayah.

Di Wilayah lain, daftar temuan untuk integrasi hanya berisi temuan dari Wilayah saat ini.

Untuk informasi tentang cara mengkonfigurasi agregasi lintas wilayah, lihatthe section called “Menggabungkan data di seluruh Wilayah”.

Dari daftar temuan, Anda dapat melakukan tindakan berikut.

- Ubah filter dan pengelompokan untuk daftar

- Lihat detail untuk temuan individu
- Memperbarui status alur kerja temuan
- Kirim temuan ke tindakan khusus

Layanan AWS integrasi dengan Security Hub CSPM

AWS Security Hub CSPM mendukung integrasi dengan beberapa lainnya. Layanan AWS Integrasi ini dapat membantu Anda mendapatkan pandangan komprehensif tentang keamanan dan kepatuhan di seluruh AWS lingkungan Anda.

Kecuali dinyatakan lain di bawah ini, Layanan AWS integrasi yang mengirimkan temuan ke Security Hub CSPM diaktifkan secara otomatis setelah Anda mengaktifkan Security Hub CSPM dan layanan lainnya. Integrasi yang menerima temuan CSPM Security Hub mungkin memerlukan langkah tambahan untuk aktivasi. Tinjau informasi tentang setiap integrasi untuk mempelajari lebih lanjut.

Beberapa integrasi tidak tersedia di semua Wilayah AWS. Pada konsol CSPM Security Hub, integrasi tidak muncul di halaman Integrasi jika tidak didukung di Wilayah saat ini. Untuk daftar integrasi yang tersedia di Wilayah China dan AWS GovCloud (US) Regions, lihatKetersediaan integrasi menurut Wilayah.

Ikhtisar dari AWS integrasi layanan dengan Security Hub CSPM

Tabel berikut memberikan gambaran umum AWS layanan yang mengirimkan temuan ke Security Hub CSPM atau menerima temuan dari Security Hub CSPM.

AWS Layanan terintegrasi	Arahan
AWS Config	Mengirim temuan
AWS Firewall Manager	Mengirim temuan
Amazon GuardDuty	Mengirim temuan
AWS Health	Mengirim temuan
AWS Identity and Access Management Access Analyzer	Mengirim temuan
Amazon Inspector	Mengirim temuan

AWS Layanan terintegrasi	Arahan	
AWS IoT Device Defender	Mengirim temuan	
Amazon Macie	Mengirim temuan	
Amazon Route 53 Resolver Firewall DNS	Mengirim temuan	
AWS Systems Manager Manajer Patch	Mengirim temuan	
AWS Audit Manager	Menerima temuan	
Amazon Q Developer dalam aplikasi obrolan	Menerima temuan	
Amazon Detective	Menerima temuan	
Amazon Security Lake	Menerima temuan	
AWS Systems Manager P enjelajah dan OpsCenter	Menerima dan memperbarui temuan	
AWS Trusted Advisor	Menerima temuan	

Layanan AWS yang mengirimkan temuan ke Security Hub CSPM

Berikut ini ter Layanan AWS integrasi dengan dan dapat mengirim temuan ke Security Hub CSPM. Security Hub CSPM mengonversi temuan ke Format Penemuan AWS Keamanan.

AWS Config (Mengirim temuan)

AWS Config adalah layanan yang memungkinkan Anda menilai, mengaudit, dan mengevaluasi konfigurasi sumber AWS daya Anda. AWS Config terus memantau dan merekam konfigurasi AWS sumber daya Anda dan memungkinkan Anda untuk mengotomatiskan evaluasi konfigurasi yang direkam terhadap konfigurasi yang diinginkan.

Dengan menggunakan integrasi dengan AWS Config, Anda dapat melihat hasil evaluasi aturan terkel AWS Config ola dan kustom sebagai temuan di Security Hub CSPM. Temuan ini dapat dilihat

bersama temuan Security Hub CSPM lainnya, memberikan gambaran komprehensif tentang postur keamanan Anda.

AWS Config menggunakan Amazon EventBridge untuk mengirim evaluasi AWS Config aturan ke Security Hub CSPM. Security Hub CSPM mengubah evaluasi aturan menjadi temuan yang mengikuti Format Penemuan AWS Keamanan. Security Hub CSPM kemudian memperkaya temuan berdasarkan upaya terbaik dengan mendapatkan informasi lebih lanjut tentang sumber daya yang terkena dampak, seperti Nama Sumber Daya Amazon (ARN), tag sumber daya, dan tanggal pembuatan.

Untuk informasi selengkapnya tentang integrasi ini, lihat bagian berikut.

Bagaimana AWS Config mengirimkan temuan ke Security Hub CSPM

Semua temuan di Security Hub CSPM menggunakan format JSON standar ASFF. ASFF mencakup rincian tentang asal temuan, sumber daya yang terpengaruh, dan status temuan saat ini. AWS Config mengirimkan evaluasi aturan terkelola dan kustom ke Security Hub CSPM melalui. EventBridge Security Hub CSPM mengubah evaluasi aturan menjadi temuan yang mengikuti ASFF dan memperkaya temuan berdasarkan upaya terbaik.

Jenis-jenis temuan yang AWS Config mengirim ke Security Hub CSPM

Setelah integrasi diaktifkan, kirim AWS Config evaluasi semua aturan terkel AWS Config ola dan aturan khusus ke Security Hub CSPM. Hanya evaluasi yang dilakukan setelah Security Hub CSPM diaktifkan yang dikirim. Misalnya, evaluasi AWS Config aturan mengungkapkan lima sumber daya yang gagal. Jika Anda mengaktifkan Security Hub CSPM setelah evaluasi itu dan aturan kemudian mengungkapkan sumber daya keenam yang gagal, hanya AWS Config mengirimkan evaluasi sumber daya keenam ke CSPM Hub Keamanan.

Evaluasi dari AWS Config aturan terkait layanan, seperti yang digunakan untuk menjalankan pemeriksaan kontrol CSPM Hub Keamanan, dikecualikan. Pengecualiannya adalah temuan yang dihasilkan oleh aturan terkait layanan yang dibuat AWS Control Tower dan dikelola. AWS Config Menyertakan temuan untuk aturan ini membantu memastikan bahwa data temuan Anda mencakup hasil pemeriksaan proaktif yang dilakukan oleh AWS Control Tower.

Mengirim AWS Config temuan untuk Security Hub CSPM

Ketika integrasi diaktifkan, Security Hub CSPM akan secara otomatis menetapkan izin yang diperlukan untuk menerima temuan dari. AWS Config Security Hub CSPM menggunakan izin tingkat layanan-ke-layanan yang memberi Anda cara aman untuk mengaktifkan integrasi ini dan mengimpor temuan dari melalui Amazon. AWS Config EventBridge

Latensi untuk mengirim temuan

Saat AWS Config membuat temuan baru, Anda biasanya dapat melihat temuan di Security Hub CSPM dalam waktu lima menit.

Mencoba lagi saat Security Hub CSPM tidak tersedia

AWS Config mengirimkan temuan ke Security Hub CSPM berdasarkan upaya terbaik melalui. EventBridge Jika acara tidak berhasil dikirim ke Security Hub CSPM, coba lagi EventBridge pengiriman hingga 24 jam atau 185 kali, mana saja yang lebih dulu.

Memperbarui yang ada AWS Config temuan di Security Hub CSPM

Setelah AWS Config mengirimkan temuan ke Security Hub CSPM, ia dapat mengirim pembaruan ke temuan yang sama ke Security Hub CSPM untuk mencerminkan pengamatan tambahan dari aktivitas temuan. Pembaruan hanya dikirim untuk `ComplianceChangeNotification` acara. Jika tidak terjadi perubahan kepatuhan, pembaruan tidak dikirim ke Security Hub CSPM. Security Hub CSPM menghapus temuan 90 hari setelah pembaruan terbaru atau 90 hari setelah pembuatan jika tidak ada pembaruan yang terjadi.

Security Hub CSPM tidak mengarsipkan temuan yang dikirim AWS Config bahkan jika Anda menghapus sumber daya terkait.

Wilayah di mana AWS Config temuan ada

AWS Config Penemuan terjadi secara regional. AWS Config mengirimkan temuan ke Security Hub CSPM di Wilayah atau Wilayah yang sama di mana temuan terjadi.

Melihat AWS Config temuan di Security Hub CSPM

Untuk melihat AWS Config temuan Anda, pilih Temuan dari panel navigasi CSPM Hub Keamanan. Untuk memfilter temuan agar hanya menampilkan AWS Config temuan, pilih Nama Produk di bilah pencarian drop-down. Masukkan Config, dan pilih Ap ply.

Menafsirkan AWS Config menemukan nama di Security Hub CSPM

Security Hub CSPM mengubah evaluasi AWS Config aturan menjadi temuan yang mengikuti. AWS Format Penemuan Keamanan (ASFF) AWS Config evaluasi aturan menggunakan pola peristiwa yang berbeda dibandingkan dengan ASFF. Tabel berikut memetakan bidang evaluasi AWS Config aturan dengan rekan ASFF mereka seperti yang muncul di Security Hub CSPM.

Jenis pencarian evaluasi aturan konfigurasi	Tipe temuan ASFF	Nilai hardcode
detail.aws AccountId	AwsAccountId	
detail.baru EvaluationResult.resultRecordedTime	CreatedAt	
detail.baru EvaluationResult.resultRecordedTime	UpdatedAt	
	ProductArn	<region>“arn ::securityhub:<partition>:: /konfigurasi” product/aws
	ProductName	“Konfigurasi”
	CompanyName	"AWS"
	Region	“eu-sentral-1"
konfigurasi RuleArn	GeneratorId, ProductFields	
detail. ConfigRuleARN/finding/hash	Id	
detail.config RuleName	Judul, ProductFields	
detail.config RuleName	Deskripsi	“Temuan ini dibuat untuk perubahan kepatuhan sumber daya untuk aturan konfigurasi:`${detail.ConfigRuleName}` ”
Item Konfigurasi “ARN” atau Hub Keamanan CSPM menghitung ARN	Sumber daya [i] .id	
Detail.ResourceType	Sumber daya [i] .Jenis	"AwsS3Bucket"

Jenis pencarian evaluasi aturan konfigurasi	Tipe temuan ASFF	Nilai hardcode
	Sumber Daya [i] .Partisi	"aws"
	Sumber daya [i] .Wilayah	“eu-sentral-1"
Item Konfigurasi “konfigurasi”	Sumber Daya [i] .Detail	
	SchemaVersion	“2018-10-08"
	Severity.Label	Lihat “Menafsirkan Label Tingkat Keparahan” di bawah ini
	Tipe	["Pemeriksaan Perangkat Lunak dan Konfigurasi"]
detail.baru EvaluationResult.complianceType	Compliance.Status	“GAGAL”, “NOT_AVAILABLE”, “LULUS”, atau “PERINGATAN”
	Workflow.Status	“DISELESAIKAN” jika AWS Config temuan dihasilkan dengan “ Compliance.Status PASSED”, atau jika Compliance.Status berubah dari “GAGAL” menjadi “PASSED.” Jika tidak, Workflow.Status akan menjadi “BARU.” Anda dapat mengubah nilai ini dengan operasi BatchUpdateFindings API.

Menafsirkan label keparahan

Semua temuan dari evaluasi AWS Config aturan memiliki label tingkat keparahan default MEDIUM di ASFF. Anda dapat memperbarui label keparahan temuan dengan operasi `BatchUpdateFindings` API.

Temuan khas dari AWS Config

Security Hub CSPM mengubah evaluasi AWS Config aturan menjadi temuan yang mengikuti ASFF. Berikut ini adalah contoh temuan khas dari AWS Config ASFF.

> **Note**
>
> Jika deskripsi lebih dari 1.024 karakter, itu akan dipotong menjadi 1.024 karakter dan akan mengatakan "(terpotong)" di akhir.

```
{
 "SchemaVersion": "2018-10-08",
 "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
 "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
 "ProductName": "Config",
 "CompanyName": "AWS",
 "Region": "eu-central-1",
 "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-
mburzq",
 "AwsAccountId": "123456789012",
 "Types": [
  "Software and Configuration Checks"
 ],
 "CreatedAt": "2022-04-15T05:00:37.181Z",
 "UpdatedAt": "2022-04-19T21:20:15.056Z",
 "Severity": {
  "Label": "MEDIUM",
  "Normalized": 40
 },
 "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
 "Description": "This finding is created for a resource compliance change for config
 rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
 "ProductFields": {
  "aws/securityhub/ProductName": "Config",
```

```
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
  "aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
  "aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
  "aws/config/ConfigComplianceType": "NON_COMPLIANT"
 },
 "Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::amzn-s3-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
   "AwsS3Bucket": {
    "OwnerId": "4edbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
    "CreatedAt": "2022-04-15T04:32:53.000Z"
   }
  }
 }],
 "Compliance": {
  "Status": "FAILED"
 },
 "WorkflowState": "NEW",
 "Workflow": {
  "Status": "NEW"
 },
 "RecordState": "ACTIVE",
 "FindingProviderFields": {
  "Severity": {
   "Label": "MEDIUM"
  },
  "Types": [
   "Software and Configuration Checks"
  ]
 }
}
```

Mengaktifkan dan mengonfigurasi integrasi

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini diaktifkan secara otomatis. AWS Config segera mulai mengirim temuan ke Security Hub CSPM.

Menghentikan publikasi temuan ke Security Hub CSPM

Untuk menghentikan pengiriman temuan ke Security Hub CSPM, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Untuk petunjuk tentang menghentikan aliran temuan, lihatMengaktifkan aliran temuan dari integrasi CSPM Security Hub.

AWS Firewall Manager (Mengirim temuan)

Firewall Manager mengirimkan temuan ke Security Hub CSPM ketika kebijakan firewall aplikasi web (WAF) untuk sumber daya atau aturan daftar kontrol akses web (ACL) tidak sesuai. Firewall Manager juga mengirimkan temuan ketika AWS Shield Advanced tidak melindungi sumber daya, atau ketika serangan diidentifikasi.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini secara otomatis diaktifkan. Firewall Manager segera mulai mengirim temuan ke Security Hub CSPM.

Untuk mempelajari lebih lanjut tentang integrasi, lihat halaman Integrasi di konsol CSPM Hub Keamanan.

Untuk mempelajari selengkapnya tentang Firewall Manager, lihat Panduan Peng AWS WAF embang .

Amazon GuardDuty (Mengirim temuan)

GuardDuty mengirimkan semua jenis temuan yang dihasilkannya ke Security Hub CSPM. Beberapa jenis temuan memiliki prasyarat, persyaratan pengaktifan, atau batasan Regional. Untuk informasi selengkapnya, lihat GuardDuty menemukan jenis di Panduan GuardDuty Pengguna Amazon.

Temuan baru dari GuardDuty dikirim ke Security Hub CSPM dalam waktu lima menit. Pembaruan temuan dikirim berdasarkan pengaturan Temuan yang diperbarui untuk Amazon EventBridge di GuardDuty pengaturan.

Saat Anda menghasilkan temuan GuardDuty sampel menggunakan halaman GuardDuty Pengaturan, Security Hub CSPM menerima temuan sampel dan menghilangkan awalan `[Sample]`

dalam jenis temuan. Misalnya, jenis pencarian sampel GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions` ditampilkan seperti `Recon:IAMUser/ResourcePermissions` di Security Hub CSPM.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini secara otomatis diaktifkan. GuardDutysegera mulai mengirim temuan ke Security Hub CSPM.

Untuk informasi selengkapnya tentang GuardDuty integrasi, lihat Meng integrasikan dengan AWS Security Hub CSPM di Panduan GuardDuty Pengguna Amazon.

AWS Health (Mengirim temuan)

AWS Health memberikan visibilitas berkelanjutan ke dalam kinerja sumber daya Anda dan ketersediaan Layanan AWS dan Anda Akun AWS. Anda dapat menggunakan AWS Health peristiwa untuk mempelajari bagaimana perubahan layanan dan sumber daya dapat memengaruhi aplikasi Anda yang berjalan AWS.

Integrasi dengan AWS Health tidak menggunakan`BatchImportFindings`. Sebagai gantinya, AWS Health gunakan pesan peristiwa layanan-ke-layanan untuk mengirim temuan ke Security Hub CSPM.

Untuk informasi selengkapnya tentang integrasi, lihat bagian berikut.

Bagaimana AWS Health mengirimkan temuan ke Security Hub CSPM

Di Security Hub CSPM, masalah keamanan dilacak sebagai temuan. Beberapa temuan berasal dari masalah yang terdeteksi oleh AWS layanan lain atau oleh mitra pihak ketiga. Security Hub CSPM juga memiliki seperangkat aturan yang digunakan untuk mendeteksi masalah keamanan dan menghasilkan temuan.

Security Hub CSPM menyediakan alat untuk mengelola temuan dari semua sumber ini. Anda dapat melihat dan memfilter daftar temuan dan melihat detail untuk temuan. Lihat Meninjau detail dan riwayat temuan di Security Hub CSPM. Anda juga dapat melacak status penyelidikan ke temuan. Lihat Mengatur status alur kerja temuan di Security Hub CSPM.

Semua temuan di Security Hub CSPM menggunakan format JSON standar yang disebut. AWS Format Penemuan Keamanan (ASFF) ASFF mencakup rincian tentang sumber masalah, sumber daya yang terpengaruh, dan status temuan saat ini.

AWS Health adalah salah satu AWS layanan yang mengirimkan temuan ke Security Hub CSPM.

Jenis-jenis temuan yang AWS Health mengirim ke Security Hub CSPM

Setelah integrasi diaktifkan, kirim AWS Health temuan yang memenuhi satu atau lebih spesifikasi yang tercantum ke Security Hub CSPM. Security Hub CSPM mencerna temuan di. AWS Format Penemuan Keamanan (ASFF)

- Temuan yang berisi salah satu nilai berikut untuk Layanan AWS:
  - RISK
  - ABUSE
  - ACM
  - CLOUDHSM
  - CLOUDTRAIL
  - CONFIG
  - CONTROLTOWER
  - DETECTIVE
  - EVENTS
  - GUARDDUTY
  - IAM
  - INSPECTOR
  - KMS
  - MACIE
  - SES
  - SECURITYHUB
  - SHIELD
  - SSO
  - COGNITO
  - IOTDEVICEDEFENDER
  - NETWORKFIREWALL
  - ROUTE53
  - WAF
  - FIREWALLMANAGER
  - SECRETSMANAGER

- BACKUP
- AUDITMANAGER
- ARTIFACT
- CLOUDENDURE
- CODEGURU
- ORGANIZATIONS
- DIRECTORYSERVICE
- RESOURCEMANAGER
- CLOUDWATCH
- DRS
- INSPECTOR2
- RESILIENCEHUB

- Temuan dengan kata-kata `securityabuse`,, atau `certificate` di AWS Health `typeCode` lapangan
- Temuan di mana AWS Health layanan berada `risk` atau `abuse`

Mengirim AWS Health temuan untuk Security Hub CSPM

Ketika Anda memilih untuk menerima temuan dari AWS Health, Security Hub CSPM akan secara otomatis menetapkan izin yang diperlukan untuk menerima temuan dari. AWS Health Security Hub CSPM menggunakan izin tingkat layanan-ke-layanan yang memberi Anda cara yang aman dan mudah untuk mengaktifkan integrasi ini dan mengimpor temuan dari AWS Health melalui Amazon atas nama Anda. EventBridge Memilih Terima Temuan memberikan izin CSPM Security Hub untuk mengkonsumsi temuan dari. AWS Health

Latensi untuk mengirim temuan

Saat AWS Health membuat temuan baru, biasanya dikirim ke Security Hub CSPM dalam waktu lima menit.

Mencoba lagi saat Security Hub CSPM tidak tersedia

AWS Health mengirimkan temuan ke Security Hub CSPM berdasarkan upaya terbaik melalui. EventBridge Jika acara tidak berhasil dikirim ke Security Hub CSPM, coba lagi EventBridge mengirim acara selama 24 jam.

Memperbarui temuan yang ada di Security Hub CSPM

Setelah AWS Health mengirimkan temuan ke Security Hub CSPM, ia dapat mengirim pembaruan ke temuan yang sama untuk mencerminkan pengamatan tambahan dari aktivitas penemuan ke Security Hub CSPM.

Wilayah di mana temuan ada

Untuk acara global, kirim tem AWS Health uan ke Security Hub CSPM di us-east-1 (AWS partisi), cn-northwest-1 (partisi China), dan gov-us-west-1 (partisi). GovCloud AWS Health mengirimkan Region-specific peristiwa ke Security Hub CSPM di Wilayah atau Wilayah yang sama tempat kejadian terjadi.

Melihat AWS Health temuan di Security Hub CSPM

Untuk melihat AWS Health temuan Anda di Security Hub CSPM, pilih Temuan dari panel navigasi. Untuk menyaring temuan agar hanya menampilkan AWS Health temuan, pilih Kesehatan dari bidang Nama Produk.

Menafsirkan AWS Health menemukan nama di Security Hub CSPM

AWS Health mengirimkan temuan ke Security Hub CSPM menggunakan. AWS Format Penemuan Keamanan (ASFF) AWS Health penemuan menggunakan pola peristiwa yang berbeda dibandingkan dengan format ASFF Security Hub CSPM. Tabel di bawah ini merinci semua bidang AWS Health temuan dengan rekan ASFF mereka seperti yang muncul di Security Hub CSPM.

Jenis temuan kesehatan	Tipe temuan ASFF	Nilai hardcode
akun	AwsAccountId	
Detail.Waktu mulai	CreatedAt	
detail.event Description.latest Description	Deskripsi	
detail.event TypeCode	GeneratorId	
Detail.eventarn (termasuk akun) + hash dari Detail.st artTime	Id	

Jenis temuan kesehatan	Tipe temuan ASFF	Nilai hardcode
<region>“arn: aws:securityhub::: /kesehatan” product/aws	ProductArn	
akun atau ResourceID	Sumber daya [i] .id	
	Sumber daya [i] .Jenis	“Lainnya”
	SchemaVersion	“2018-10-08"
	Severity.Label	Lihat “Menafsirkan Label Tingkat Keparahan” di bawah ini
“AWS Health -” detail.event TypeCode	judul	
-	Tipe	["Pemeriksaan Perangkat Lunak dan Konfigurasi"]
waktu acara	UpdatedAt	
URL acara di konsol Kesehatan	SourceUrl	

Menafsirkan label keparahan

Label keparahan dalam temuan ASFF ditentukan menggunakan logika berikut:

- Tingkat keparahan KRI TIS jika:
  - `service`Bidang dalam AWS Health temuan memiliki nilai `Risk`
  - `typeCode`Bidang dalam AWS Health temuan memiliki nilai `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`
  - `typeCode`Bidang dalam AWS Health temuan memiliki nilai `AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK`

- `typeCode`Bidang dalam AWS Health temuan memiliki nilai `AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES`

Tingkat keparahan TINGGI jika:

- `service`Bidang dalam AWS Health temuan memiliki nilai `Abuse`
- `typeCode`Bidang dalam AWS Health temuan berisi nilai `SECURITY_NOTIFICATION`
- `typeCode`Bidang dalam AWS Health temuan berisi nilai `ABUSE_DETECTION`

Tingkat keparahan MEDIUM jika:

- Bid `service` ang dalam temuan adalah salah satu dari berikut ini:`ACM`,`ARTIFACT`,`AUDITMANAGER`,`BACKUP`,`CLOUDENDURE`,`CLOUDHSM`,`CLOUDTRAIL`,`CLOUDWATCH`,`COD` atau `WAF`
- Bid ang TypeCode dalam tem AWS Health uan berisi nilai `CERTIFICATE`
- Bid ang TypeCode dalam tem AWS Health uan berisi nilai `END_OF_SUPPORT`

Temuan khas dari AWS Health

AWS Health mengirimkan temuan ke Security Hub CSPM menggunakan. AWS Format Penemuan Keamanan (ASFF) Berikut ini adalah contoh temuan khas dari AWS Health.

> **Note**
>
> Jika deskripsi lebih dari 1024 karakter, itu akan dipotong menjadi 1024 karakter dan akan mengatakan (terpotong) di akhir.

```
{
            "SchemaVersion": "2018-10-08",
            "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
            "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
            "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
            "AwsAccountId": "123456789012",
            "Types": [
                "Software and Configuration Checks"
            ],
```

```
            "CreatedAt": "2022-01-07T16:34:04.000Z",
            "UpdatedAt": "2022-01-07T19:17:43.000Z",
            "Severity": {
                "Label": "MEDIUM",
                "Normalized": 40
            },
            "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
            "Description": "Congratulations! Amazon SES has successfully detected the
 MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\\n\\nYou can now use this MAIL
 FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
 that is configured to use it. For information about how to configure a verified
 identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\\n\\nPlease note that this email only applies to
 AWS Region US East (N. Virginia).",
            "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
            "ProductFields": {
                "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
                "aws/securityhub/ProductName": "Health",
                "aws/securityhub/CompanyName": "AWS"
            },
            "Resources": [
                {
                    "Type": "Other",
                    "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
                }
            ],
            "WorkflowState": "NEW",
            "Workflow": {
                "Status": "NEW"
            },
            "RecordState": "ACTIVE",
            "FindingProviderFields": {
                "Severity": {
                    "Label": "MEDIUM"
                },
                "Types": [
                    "Software and Configuration Checks"
```

```
                ]
            }
        }
    ]
}
```

Mengaktifkan dan mengonfigurasi integrasi

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini secara otomatis diaktifkan. AWS Health segera mulai mengirim temuan ke Security Hub CSPM.

Menghentikan publikasi temuan ke Security Hub CSPM

Untuk menghentikan pengiriman temuan ke Security Hub CSPM, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API.

Untuk petunjuk tentang menghentikan aliran temuan, lihatMengaktifkan aliran temuan dari integrasi CSPM Security Hub.

AWS Identity and Access Management Access Analyzer (Mengirim temuan)

Dengan IAM Access Analyzer, semua temuan dikirim ke Security Hub CSPM.

IAM Access Analyzer menggunakan penalaran berbasis logika untuk menganalisis kebijakan berbasis sumber daya yang diterapkan ke sumber daya yang didukung di akun Anda. IAM Access Analyzer menghasilkan temuan ketika mendeteksi pernyataan kebijakan yang memungkinkan prinsipal eksternal mengakses sumber daya di akun Anda.

Di IAM Access Analyzer, hanya akun administrator yang dapat melihat temuan untuk penganalisis yang berlaku untuk organisasi. Untuk penganalisis organisasi, bidang `AwsAccountId` ASFF mencerminkan ID akun administrator. Di bawah`ProductFields`, `ResourceOwnerAccount` bidang menunjukkan akun di mana temuan itu ditemukan. Jika Anda mengaktifkan penganalisis secara individual untuk setiap akun, Security Hub CSPM menghasilkan beberapa temuan, satu yang mengidentifikasi ID akun administrator dan satu yang mengidentifikasi ID akun sumber daya.

Untuk informasi selengkapnya, lihat Integrasi dengan AWS Security Hub CSPM di Panduan Pengguna IAM.

Amazon Inspector (Mengirim temuan)

Amazon Inspector adalah layanan manajemen kerentanan yang terus memindai AWS beban kerja Anda untuk mencari kerentanan. Amazon Inspector secara otomatis menemukan dan memindai

instans Amazon EC2 dan gambar kontainer yang berada di Amazon Elastic Container Registry. Pemindaian mencari kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini secara otomatis diaktifkan. Amazon Inspector segera mulai mengirim semua temuan yang dihasilkannya ke Security Hub CSPM.

Untuk informasi selengkapnya tentang integrasi, lihat Integrasi dengan AWS Security Hub CSPM di Panduan Pengguna Amazon Inspector.

Security Hub CSPM juga dapat menerima temuan dari Amazon Inspector Classic. Amazon Inspector Classic mengirimkan temuan ke Security Hub CSPM yang dihasilkan melalui proses penilaian untuk semua paket aturan yang didukung.

Untuk informasi selengkapnya tentang integrasi, lihat Integrasi dengan AWS Security Hub CSPM di Panduan Pengguna Amazon Inspector Classic.

Temuan untuk Amazon Inspector dan Amazon Inspector Classic menggunakan produk yang sama ARN. Temuan Amazon Inspector memiliki entri berikut di`ProductFields`:

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> Temuan keamanan yang dihasilkan oleh Amazon Inspector Code Security tidak tersedia untuk integrasi ini. Namun, Anda dapat mengakses temuan khusus ini di konsol Amazon Inspector dan melalui Amazon Inspector API.

AWS IoT Device Defender (Mengirim temuan)

AWS IoT Device Defender adalah layanan keamanan yang mengaudit konfigurasi perangkat IoT Anda, memantau perangkat yang terhubung untuk mendeteksi perilaku abnormal, dan membantu mengurangi risiko keamanan.

Setelah mengaktifkan keduanya AWS IoT Device Defender dan Security Hub CSPM, kunjungi halaman Integrasi konsol CSPM Hub Keamanan, dan pilih Terima temuan untuk Audit, Deteksi, atau keduanya. AWS IoT Device Defender Audit dan Detect mulai mengirim semua temuan ke Security Hub CSPM.

AWS IoT Device Defender Audit mengirimkan ringkasan cek ke Security Hub CSPM, yang berisi informasi umum untuk jenis pemeriksaan audit tertentu dan tugas audit. AWS IoT Device Defender

Detect mengirimkan temuan pelanggaran untuk pembelajaran mesin (ML), statistik, dan perilaku statis ke Security Hub CSPM. Audit juga mengirimkan pembaruan pencarian ke Security Hub CSPM.

Untuk informasi selengkapnya tentang integrasi ini, lihat Integrasi dengan AWS Security Hub CSPM di Panduan Peng AWS IoT embang.

Amazon Macie (Mengirim temuan)

Amazon Macie adalah layanan keamanan data yang menemukan data sensitif dengan menggunakan machine learning dan pencocokan pola, memberikan visibilitas ke risiko keamanan data, dan memungkinkan perlindungan otomatis terhadap risiko tersebut. Temuan dari Macie dapat menunjukkan bahwa potensi pelanggaran kebijakan atau data sensitif ada di aset data Amazon S3 Anda.

Setelah Anda mengaktifkan Security Hub CSPM, Macie secara otomatis mulai mengirim temuan kebijakan ke Security Hub CSPM. Anda dapat mengonfigurasi integrasi untuk juga mengirim temuan data sensitif ke Security Hub CSPM.

Di Security Hub CSPM, jenis temuan untuk kebijakan atau temuan data sensitif diubah menjadi nilai yang kompatibel dengan ASFF. Misalnya, jenis tem `Policy:IAMUser/S3BucketPublic` uan di Macie ditampilkan seperti `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic` di Security Hub CSPM.

Macie juga mengirimkan temuan sampel yang dihasilkan ke Security Hub CSPM. Untuk temuan sampel, nama sumber daya yang terpengaruh adalah `macie-sample-finding-bucket` dan nilai untuk `Sample` bidang tersebut adalah`true`.

Untuk informasi selengkapnya, lihat Mengevaluasi temuan Macie dengan Security Hub di Panduan Pengguna Amazon Macie.

Amazon Route 53 Resolver DNS Firewall (Mengirim temuan)

Dengan Amazon Route 53 Resolver DNS Firewall, Anda dapat memfilter dan mengatur lalu lintas DNS keluar untuk cloud pribadi virtual (VPC) Anda. Anda melakukan ini dengan membuat kumpulan aturan pemfilteran yang dapat digunakan kembali di grup aturan DNS Firewall, mengaitkan grup aturan dengan VPC Anda, lalu memantau aktivitas di log dan metrik DNS Firewall. Berdasarkan aktivitas, Anda dapat menyesuaikan perilaku DNS Firewall. DNS Firewall adalah fitur dari Route 53 Resolver.

Route 53 Resolver DNS Firewall dapat mengirim beberapa jenis temuan ke Security Hub CSPM:

- Temuan terkait kueri yang diblokir atau diperingatkan untuk domain yang terkait dengan Daftar Domain Terkelola, yang merupakan daftar domain yang AWS dikelola AWS .
- Temuan terkait kueri yang diblokir atau diperingatkan untuk domain yang terkait dengan daftar domain kustom yang Anda tentukan.
- Temuan terkait kueri yang diblokir atau diperingatkan oleh DNS Firewall Advanced, yang merupakan fitur Route 53 Resolver yang dapat mendeteksi kueri yang terkait dengan ancaman DNS tingkat lanjut seperti Domain Generation Algorithms (DGA) dan DNS Tunneling.

Setelah Anda mengaktifkan Security Hub CSPM dan Route 53 Resolver DNS Firewall, DNS Firewall secara otomatis mulai mengirim temuan untuk Daftar Domain Terkel AWS ola dan DNS Firewall Advanced ke Security Hub CSPM. Untuk juga mengirim temuan untuk daftar domain kustom ke Security Hub CSPM, aktifkan integrasi secara manual di Security Hub CSPM.

Di Security Hub CSPM, semua temuan dari Route 53 Resolver DNS Firewall memiliki tipe berikut:. `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation`

Untuk informasi selengkapnya, lihat Mengirim temuan dari Route 53 Resolver DNS Firewall ke Security Hub di Panduan Pengembang Amazon Route 53.

AWS Systems Manager Patch Manager (Mengirim temuan)

AWS Systems Manager Patch Manager mengirimkan temuan ke Security Hub CSPM ketika instans dalam armada pelanggan tidak sesuai dengan standar kepatuhan patch mereka.

Patch Manager mengotomatiskan proses patching instans terkelola dengan pembaruan terkait keamanan dan jenis pembaruan lainnya.

Setelah Anda mengaktifkan Security Hub CSPM, integrasi ini secara otomatis diaktifkan. Manajer Sistem Patch Manager segera mulai mengirim temuan ke Security Hub CSPM.

Untuk informasi selengkapnya tentang menggunakan Patch Manager, lihat AWS Systems Manager Patch Manager di Panduan AWS Systems Manager Pengguna.

AWS layanan yang menerima temuan dari Security Hub CSPM

AWS Layanan berikut terintegrasi dengan Security Hub CSPM dan menerima temuan dari Security Hub CSPM. Jika dicatat, layanan terintegrasi juga dapat memperbarui temuan. Dalam hal ini, menemukan pembaruan yang Anda buat dalam layanan terintegrasi juga akan tercermin dalam Security Hub CSPM.

AWS Audit Manager (Menerima temuan)

AWS Audit Manager menerima temuan dari Security Hub CSPM. Temuan ini membantu pengguna Audit Manager mempersiapkan audit.

Untuk mempelajari lebih lanjut tentang Audit Manager, lihat Panduan AWS Pengguna Manajer Audit . AWS Pemeriksaan CSPM Hub Keamanan yang didukung oleh AWS Audit Manager daftar kontrol yang mengirimkan temuan Security Hub CSPM ke Audit Manager.

Pengembang Amazon Q dalam aplikasi obrolan (Menerima temuan)

Pengembang Amazon Q dalam aplikasi obrolan adalah agen interaktif yang membantu Anda memantau dan berinteraksi dengan AWS sumber daya Anda di saluran Slack dan ruang obrolan Amazon Chime.

Pengembang Amazon Q dalam aplikasi obrolan menerima temuan dari Security Hub CSPM.

Untuk mempelajari selengkapnya tentang Amazon Q Developer dalam integrasi aplikasi obrolan dengan Security Hub CSPM, lihat ikhtisar integrasi Security Hub CSPM di Panduan Administrator Pengembang Amazon Q di aplikasi obrolan.

Detektif Amazon (Menerima temuan)

Detective secara otomatis mengumpulkan data log dari AWS sumber daya Anda dan menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk membantu Anda memvisualisasikan dan melakukan penyelidikan keamanan yang lebih cepat dan lebih efisien.

Integrasi Security Hub CSPM dengan Detective memungkinkan Anda untuk beralih dari GuardDuty temuan Amazon di Security Hub CSPM menjadi Detective. Anda kemudian dapat menggunakan alat Detektif dan visualisasi untuk menyelidikinya. Integrasi tidak memerlukan konfigurasi tambahan apa pun di Security Hub CSPM atau Detective.

Untuk temuan yang diterima dari orang lain Layanan AWS, panel rincian temuan di konsol CSPM Security Hub mencakup subbagian Investigate in Detective. Subbagian itu berisi tautan ke Detektif di mana Anda dapat menyelidiki lebih lanjut masalah keamanan yang ditandai oleh temuan itu. Anda juga dapat membuat grafik perilaku di Detective berdasarkan temuan Security Hub CSPM untuk melakukan penyelidikan yang lebih efektif. Untuk informasi selengkapnya, lihat temuan AWS keamanan di Panduan Administrasi Detektif Amazon.

Jika agregasi lintas wilayah diaktifkan, maka ketika Anda melakukan pivot dari Wilayah agregasi, Detektif akan terbuka di Wilayah tempat temuan berasal.

Jika tautan tidak berfungsi, maka untuk saran pemecahan masalah, lihat Mem ecahkan masalah pivot.

Amazon Security Lake (Menerima temuan)

Security Lake adalah layanan danau data keamanan yang dikelola sepenuhnya. Anda dapat menggunakan Security Lake untuk secara otomatis memusatkan data keamanan dari sumber cloud, lokal, dan kustom ke dalam data lake yang disimpan di akun Anda. Pelanggan dapat menggunakan data dari Security Lake untuk kasus penggunaan investigasi dan analitik.

Untuk mengaktifkan integrasi ini, Anda harus mengaktifkan kedua layanan dan menambahkan Security Hub CSPM sebagai sumber di konsol Security Lake, Security Lake API, atau. AWS CLI Setelah Anda menyelesaikan langkah-langkah ini, Security Hub CSPM mulai mengirim semua temuan ke Security Lake.

Security Lake secara otomatis menormalkan temuan Security Hub CSPM dan mengubahnya menjadi skema open-source standar yang disebut Open Cybersecurity Schema Framework (OCSF). Di Security Lake, Anda dapat menambahkan satu atau lebih pelanggan untuk menggunakan temuan CSPM Security Hub.

Untuk informasi selengkapnya tentang integrasi ini, termasuk petunjuk tentang menambahkan Security Hub CSPM sebagai sumber dan membuat pelanggan, lihat Integrasi dengan AWS Security Hub CSPM di Panduan Pengguna Amazon Security Lake.

AWS Systems Manager Explorer dan OpsCenter (Menerima dan memperbarui temuan)

AWS Systems Manager Jelajahi dan OpsCenter terima temuan dari Security Hub CSPM, dan perbarui temuan tersebut di Security Hub CSPM.

Explorer memberi Anda dasbor yang dapat disesuaikan, memberikan wawasan dan analisis utama tentang kesehatan operasional dan kinerja AWS lingkungan Anda.

OpsCenter memberi Anda lokasi pusat untuk melihat, menyelidiki, dan menyelesaikan item pekerjaan operasional.

Untuk informasi selengkapnya tentang Explorer dan OpsCenter, lihat Manajemen operasi di Panduan AWS Systems Manager Pengguna.

AWS Trusted Advisor (Menerima temuan)

Trusted Advisor memanfaatkan praktik terbaik yang dipelajari dari melayani ratusan ribu AWS pelanggan. Trusted Advisor memeriksa AWS lingkungan Anda, dan kemudian membuat rekomendasi

ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup celah keamanan.

Saat Anda mengaktifkan keduanya Trusted Advisor dan Security Hub CSPM, integrasi diperbarui secara otomatis.

Security Hub CSPM mengirimkan hasil pemeriksaan Praktik Terbaik AWS Keamanan Dasarnya ke. Trusted Advisor

Untuk informasi selengkapnya tentang integrasi Security Hub CSPM dengan Trusted Advisor, lihat Melihat kontrol CSPM Hub AWS Keamanan AWS Trusted Advisor di Panduan Pengguna Dukungan. AWS

Third-party integrasi produk dengan Security Hub CSPM

AWS Security Hub CSPM terintegrasi dengan beberapa produk mitra pihak ketiga. Integrasi dapat melakukan satu atau lebih tindakan berikut:

- Kirim temuan yang dihasilkannya ke Security Hub CSPM
- Menerima temuan dari Security Hub CSPM
- Perbarui temuan di Security Hub CSPM

Integrasi yang mengirimkan temuan ke Security Hub CSPM memiliki Amazon Resource Name (ARN).

Integrasi mungkin tidak tersedia di semua Wilayah AWS. Jika integrasi tidak didukung di Wilayah tempat Anda saat ini masuk di konsol CSPM Hub Keamanan, integrasi tersebut tidak muncul di halaman Integrasi konsol. Untuk daftar integrasi yang tersedia di Wilayah China dan AWS GovCloud (US) Regions, lihatKetersediaan integrasi menurut Wilayah.

Jika Anda memiliki solusi keamanan dan tertarik untuk menjadi mitra Security Hub CSPM, kirim email ke < `securityhub-partners@amazon.com.` > Untuk informasi selengkapnya, lihat Panduan Integrasi Mitra.

Ikhtisar integrasi pihak ketiga dengan Security Hub CSPM

Tabel berikut memberikan gambaran umum tentang integrasi pihak ketiga yang dapat mengirimkan temuan ke Security Hub CSPM atau menerima temuan dari Security Hub CSPM.

Integrasi	Arahan	ARN (jika berlaku)
3CORESec – 3CORESec NTA	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/3coresec/3coresec`
Alert Logic – SIEMless Threat Management	Mengirim temuan	`arn:aws:securityhub: <REGION>:733251395267:product/alertlogic/althreatmanagement`
Aqua Security – Aqua Cloud Native Security Platform	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/aquasecurity/aquasecurity`
Aqua Security – Kube-bench	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench`
Armor – Armor Anywhere	Mengirim temuan	`arn:aws:securityhub: <REGION>:679703615338:product/armordefense/armoranywhere`
AttackIQ – AttackIQ	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform`
Barracuda Networks – Cloud Security Guardian	Mengirim temuan	`arn:aws:securityhub: <REGION>:151784055945:product/barra`

Integrasi	Arahan	ARN (jika berlaku)
		`cuda/cloudsecurityguardian`
BigID – BigID Enterprise	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise`
Blue Hexagon – Blue Hexagon forAWS	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws`
Check Point – CloudGuard IaaS	Mengirim temuan	`arn:aws:securityhub: <REGION>:757245563457:product/checkpoint/cloudguard-iaas`
Check Point – CloudGuard Posture Management	Mengirim temuan	`arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc`
Claroty – xDome	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/claroty/xdome`
Cloud Storage Security—Antivirus for Amazon S3	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Integrasi	Arahan	ARN (jika berlaku)
Contrast Security	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/contrast-security/security-assess`
CrowdStrike – CrowdStrike Falcon	Mengirim temuan	`arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`
CyberArk – Privileged Threat Analytics	Mengirim temuan	`arn:aws:securityhub: <REGION>:749430749651:product/cyberark/cyberark-pta`
Data Theorem – Data Theorem	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/data-theorem/api-cloud-web-secure`
Drata	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/drata/drata-integration`
Forcepoint – Forcepoint CASB	Mengirim temuan	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-casb`

Integrasi	Arahan	ARN (jika berlaku)
Forcepoint – Forcepoint Cloud Security Gateway	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/forcepoint/forcepoint-cloud-security-gateway`
Forcepoint – Forcepoint DLP	Mengirim temuan	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-dlp`
Forcepoint – Forcepoint NGFW	Mengirim temuan	`arn:aws:securityhub: <REGION>:365761988620:product/forcepoint/forcepoint-ngfw`
Fugue – Fugue	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/fugue/fugue`
Guardicore – Centra 4.0	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/guardicore/guardicore`
HackerOne – Vulnerability Intelligence	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/hackerone/vulnerability-intelligence`
JFrog – Xray	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/jfrog/jfrog-xray`

Integrasi	Arahan	ARN (jika berlaku)
Juniper Networks – vSRX Next Generation Firewall	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/juniper-networks/vsrx-next-generation-firewall`
k9 Security – Access Analyzer	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/k9-security/access-analyzer`
Lacework – Lacework	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/lacework/lacework`
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`
NETSCOUT – NETSCOUT Cyber Investigator	Mengirim temuan	`arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator`
Orca Cloud Security Platform	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/orca-security/orca-security`

Integrasi	Arahan	ARN (jika berlaku)
Palo Alto Networks – Prisma Cloud Compute	Mengirim temuan	`arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise`
Palo Alto Networks – Prisma Cloud Enterprise	Mengirim temuan	`arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock`
Plerion – Cloud Security Platform	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform`
Prowler – Prowler	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/prowler/prowler`
Qualys – Vulnerability Management	Mengirim temuan	`arn:aws:securityhub: <REGION>:805950163170:product/qualys/qualys-vm`
Rapid7 – InsightVM	Mengirim temuan	`arn:aws:securityhub: <REGION>:336818582268:product/rapid7/insightvm`
SentinelOne – SentinelOne	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/sentinelone/endpoint-protection`

Integrasi	Arahan	ARN (jika berlaku)
Snyk	Mengirim temuan	`arn:aws:securityhub: <region>::product/snyk/snyk`
Sonrai Security – Sonrai Dig	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/sonrai-security/sonrai-dig`
Sophos – Server Protection	Mengirim temuan	`arn:aws:securityhub: <REGION>:062897671886:product/sophos/sophos-server-protection`
StackRox – StackRox Kubernetes Security	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security`
Sumo Logic – Machine Data Analytics	Mengirim temuan	`arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda`
Symantec – Cloud Workload Protection	Mengirim temuan	`arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp`
Tenable – Tenable.io	Mengirim temuan	`arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io`

Integrasi	Arahan	ARN (jika berlaku)
Trend Micro – Cloud One	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one`
Vectra – Cognito Detect	Mengirim temuan	`arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect`
Wiz	Mengirim temuan	`arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security`
Atlassian - Jira Service Management	Menerima dan memperbarui temuan	Tidak berlaku
Atlassian - Jira Service Management Cloud	Menerima dan memperbarui temuan	Tidak berlaku
Atlassian – Opsgenie	Menerima temuan	Tidak berlaku
Dynatrace	Menerima temuan	Tidak berlaku
Elastic	Menerima temuan	Tidak berlaku
Fortinet – FortiCNP	Menerima temuan	Tidak berlaku
IBM – QRadar	Menerima temuan	Tidak berlaku
Logz.io Cloud SIEM	Menerima temuan	Tidak berlaku
MetricStream	Menerima temuan	Tidak berlaku
MicroFocus – MicroFocus Arcsight	Menerima temuan	Tidak berlaku

Integrasi	Arahan	ARN (jika berlaku)
New Relic Vulnerability Management	Menerima temuan	Tidak berlaku
PagerDuty – PagerDuty	Menerima temuan	Tidak berlaku
Palo Alto Networks – Cortex XSOAR	Menerima temuan	Tidak berlaku
Palo Alto Networks – VM-Series	Menerima temuan	Tidak berlaku
Rackspace Technology – Cloud Native Security	Menerima temuan	Tidak berlaku
Rapid7 – InsightConnect	Menerima temuan	Tidak berlaku
RSA – RSA Archer	Menerima temuan	Tidak berlaku
ServiceNow – ITSM	Menerima dan memperbarui temuan	Tidak berlaku
Slack – Slack	Menerima temuan	Tidak berlaku
Splunk – Splunk Enterprise	Menerima temuan	Tidak berlaku
Splunk – Splunk Phantom	Menerima temuan	Tidak berlaku
ThreatModeler	Menerima temuan	Tidak berlaku
Trellix – Trellix Helix	Menerima temuan	Tidak berlaku
Caveonix – Caveonix Cloud	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud`

Integrasi	Arahan	ARN (jika berlaku)
Cloud Custodian – Cloud Custodian	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian`
DisruptOps, Inc. – DisruptOPS	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops`
Kion	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio`
Turbot – Turbot	Mengirim dan menerima temuan	`arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot`

Third-party integrasi yang mengirimkan temuan ke Security Hub CSPM

Integrasi produk mitra pihak ketiga berikut dapat mengirimkan temuan ke Security Hub CSPM. Security Hub CSPM mengubah temuan menjadi Format Penemuan AWS Keamanan.

3CoreSEC – 3CoreSEC NTA

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESecmenyediakan layanan deteksi terkelola untuk lokal dan AWS sistem. Integrasi mereka dengan Security Hub CSPM memungkinkan visibilitas ke dalam ancaman seperti malware, eskalasi hak istimewa, pergerakan lateral, dan segmentasi jaringan yang tidak tepat.

Tautan produk

Dokumentasi mitra

Logika Peringatan – Manajemen Ancaman SieMless

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Dapatkan tingkat cakupan yang tepat: kerentanan dan visibilitas aset, deteksi ancaman dan manajemen insiden AWS WAF, dan opsi analis SOC yang ditugaskan.

Tautan produk

Dokumentasi mitra

Keamanan Aqua – Platform Keamanan Asli Aqua Cloud

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)menyediakan keamanan siklus hidup penuh untuk aplikasi berbasis container dan tanpa server, dari CI/CD pipeline Anda hingga lingkungan produksi runtime.

Tautan produk

Dokumentasi mitra

Keamanan Aqua – Kube-bench

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-benchadalah alat sumber terbuka yang menjalankan Pusat Keamanan Internet (CIS) Kubernetes Benchmark terhadap lingkungan Anda.

Tautan produk

Dokumentasi mitra

Armor – Armor Dimana Saja

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywherememberikan keamanan dan kepatuhan terkelola untuk AWS.

Tautan produk

Dokumentasi mitra

AttackQ – AttackQ

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platformmeniru perilaku permusuhan nyata yang selaras dengan Kerangka Kerja MITRE ATT&CK untuk membantu memvalidasi dan meningkatkan postur keamanan Anda secara keseluruhan.

Tautan produk

Dokumentasi mitra

Jaringan Barracuda – Penjaga Keamanan Cloud

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentrymembantu organisasi tetap aman saat membangun aplikasi di, dan memindahkan beban kerja ke, cloud publik.

AWS Tautan pasar

Tautan produk

BigID – Perusahaan BigID

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

Ini BigID Enterprise Privacy Management Platform membantu perusahaan mengelola dan melindungi data sensitif (PII) di semua sistem mereka.

Tautan produk

Dokumentasi mitra

Biru segi enam – Biru segi enam untuk AWS

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagonadalah platform deteksi ancaman waktu nyata. Ini menggunakan prinsip pembelajaran mendalam untuk mendeteksi ancaman yang diketahui dan tidak diketahui, termasuk malware dan anomali jaringan.

AWS Tautan pasar

Dokumentasi mitra

Titik Pemeriksaan – CloudGuard IaaS

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuarddengan mudah memperluas keamanan pencegahan ancaman komprehensif AWS sambil melindungi aset di cloud.

Tautan produk

Dokumentasi mitra

Titik Pemeriksaan – CloudGuard Manajemen Postur

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Platform SaaS yang memberikan keamanan jaringan cloud yang dapat diverifikasi, perlindungan IAM tingkat lanjut, dan kepatuhan dan tata kelola yang komprehensif.

Tautan produk

Dokumentasi mitra

Claroty – XDome

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDomemembantu organisasi mengamankan sistem cyber-fisik mereka di Extended Internet of Things (XioT) dalam lingkungan industri (OT), perawatan kesehatan (IoMT), dan perusahaan (IoT).

Tautan produk

Dokumentasi mitra

Keamanan Penyimpanan Cloud – Antivirus untuk Amazon S3

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Securitymenyediakan pemindaian anti-malware dan antivirus asli cloud untuk objek Amazon S3.

Antivirus for Amazon S3 menawarkan pemindaian objek dan file secara real time dan terjadwal di Amazon S3 untuk malware dan ancaman. Ini memberikan visibilitas dan remediasi untuk masalah dan file yang terinfeksi.

Tautan produk

Dokumentasi mitra

Keamanan Kontras — Penilaian Kontras

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assessadalah alat IAST yang menawarkan deteksi kerentanan real-time di aplikasi web, API, dan layanan mikro. Contrast Assessterintegrasi dengan Security Hub CSPM untuk membantu memberikan visibilitas dan respons terpusat untuk semua beban kerja Anda.

Tautan produk

Dokumentasi mitra

CrowdStrike – CrowdStrike Elang

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Sensor CrowdStrike Falcon tunggal yang ringan menyatukan antivirus generasi berikutnya, deteksi dan respons titik akhir, serta pencarian ter 24/7 kelola melalui cloud.

AWS Tautan pasar

Dokumentasi mitra

CyberArk – Analisis Ancaman Istimewa

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analyticsmengumpulkan, mendeteksi, memperingatkan, dan menanggapi aktivitas berisiko tinggi dan perilaku akun istimewa untuk menahan serangan yang sedang berlangsung.

Tautan produk

Dokumentasi mitra

Teorema Data – Teorema Data

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theoremterus memindai aplikasi web, API, dan sumber daya cloud untuk mencari kelemahan keamanan dan celah privasi data untuk mencegah pelanggaran AppSec data.

Tautan produk

Dokumentasi mitra

Drata

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drataadalah platform otomatisasi kepatuhan yang membantu Anda mencapai dan mempertahankan kepatuhan dengan berbagai kerangka kerja, seperti SOC2, ISO, dan GDPR. Integrasi antara Drata dan Security Hub CSPM membantu Anda memusatkan temuan keamanan Anda di satu lokasi.

AWS Tautan pasar

Dokumentasi mitra

Titik kekuatan – Titik kekuatan CASB

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASBmemungkinkan Anda menemukan penggunaan aplikasi cloud, menganalisis risiko, dan menerapkan kontrol yang sesuai untuk SaaS dan aplikasi khusus.

Tautan produk

Dokumentasi mitra

Titik kekuatan – Gerbang Keamanan Cloud Forcepoint

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gatewayadalah layanan keamanan cloud konvergen yang menyediakan visibilitas, kontrol, dan perlindungan ancaman bagi pengguna dan data, di mana pun mereka berada.

Tautan produk

Dokumentasi mitra

Titik kekuatan – Titik kekuatan DLP

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLPmengatasi risiko yang berpusat pada manusia dengan visibilitas dan kontrol di mana pun karyawan Anda bekerja dan di mana pun data Anda berada.

Tautan produk

Dokumentasi mitra

Titik kekuatan – Titik kekuatan NGFW

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWmemungkinkan Anda menghubungkan AWS lingkungan Anda ke jaringan perusahaan Anda dengan skalabilitas, perlindungan, dan wawasan yang diperlukan untuk mengelola jaringan Anda dan menanggapi ancaman.

Tautan produk

Dokumentasi mitra

Fuga – Fuga

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueadalah platform cloud-native yang dapat diskalakan tanpa agen yang mengotomatiskan validasi berkelanjutan dari infrastruktur sebagai kode dan lingkungan runtime cloud menggunakan kebijakan yang sama.

Tautan produk

Dokumentasi mitra

Penjaga – Pusat 4.0

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centramenyediakan visualisasi aliran, segmentasi mikro, dan deteksi pelanggaran untuk beban kerja di pusat data modern dan cloud.

Tautan produk

Dokumentasi mitra

HackerOne – Intelijen Kerentanan

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

HackerOnePlatform ini bermitra dengan komunitas peretas global untuk mengungkap masalah keamanan yang paling relevan. Vulnerability Intelligencememungkinkan organisasi Anda melampaui pemindaian otomatis. Ini berbagi kerentanan yang telah divalidasi oleh peretas HackerOne etis dan memberikan langkah-langkah untuk mereproduksi.

AWS tautan pasar

Dokumentasi mitra

JFrog – Sinar X

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xrayadalah alat Analisis Komposisi Perangkat Lunak (SCA) keamanan aplikasi universal yang terus memindai binari untuk kepatuhan lisensi dan kerentanan keamanan sehingga Anda dapat menjalankan rantai pasokan perangkat lunak yang aman.

AWS Tautan pasar

Dokumentasi mitra

Jaringan Juniper – Firewall Generasi Berikutnya VSRx

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'VSRx Virtual Next Generation Firewall menghadirkan firewall virtual berbasis cloud lengkap dengan keamanan canggih, jaringan yang aman, kuat SD-WAN, dan otomatisasi bawaan.

AWS Tautan pasar

Dokumentasi mitra

Tautan produk

K9 Keamanan – Penganalisis Akses

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Securitymemberi tahu Anda ketika perubahan akses penting terjadi di AWS Identity and Access Management akun Anda. Dengank9 Security, Anda dapat memahami akses yang dimiliki pengguna dan peran IAM ke kritis Layanan AWS dan data Anda.

k9 Securitydibangun untuk pengiriman berkelanjutan, memungkinkan Anda untuk mengoperasionalkan IAM dengan audit akses yang dapat ditindaklanjuti dan otomatisasi kebijakan sederhana untuk AWS CDK dan Terraform.

Tautan produk

Dokumentasi mitra

Renda – Renda

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Laceworkadalah platform keamanan berbasis data untuk cloud. Platform Keamanan Cloud Lacework mengotomatiskan keamanan cloud dalam skala besar sehingga Anda dapat berinovasi dengan kecepatan dan keamanan.

Tautan produk

Dokumentasi mitra

McAfee – Platform Perlindungan Aplikasi Asli MVISION Cloud (CNAPP)

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)menawarkan Cloud Security Posture Management (CSPM) dan Cloud Workload Protection Platform (CWPP) untuk lingkungan Anda. AWS

Tautan produk

Dokumentasi mitra

NETSCOUT – Penyelidik Cyber NETSCOUT

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigatoradalah platform ancaman jaringan, investigasi risiko, dan analisis forensik di seluruh perusahaan yang membantu mengurangi dampak ancaman cyber pada bisnis.

Tautan produk

Dokumentasi mitra

Platform Keamanan Cloud Orca

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Ini Orca Cloud Security Platform mengidentifikasi, memprioritaskan, dan memperbaiki risiko dan masalah kepatuhan di seluruh cloud estate Anda. Orca'sagentless-first, AI-driven platform menawarkan cakupan komprehensif yang mendeteksi kerentanan, kesalahan konfigurasi, pergerakan lateral, risiko API, data sensitif, peristiwa dan perilaku anomali, dan identitas yang terlalu permisif.

Orcaterintegrasi dengan Security Hub CSPM untuk membawa telemetri keamanan cloud yang mendalam ke dalam Security Hub CSPM. Orca, menggunakan SideScanning teknologinya, memprioritaskan risiko di seluruh infrastruktur cloud, beban kerja, aplikasi, data, API, identitas, dan banyak lagi.

Tautan produk

Dokumentasi mitra

Jaringan Palo Alto – Komputasi Awan Prisma

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Computeadalah platform keamanan siber asli cloud yang melindungi VM, kontainer, dan platform tanpa server.

Tautan produk

Dokumentasi mitra

Jaringan Palo Alto – Perusahaan Awan Prisma

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Melindungi AWS penerapan Anda dengan analisis keamanan cloud, deteksi ancaman tingkat lanjut, dan pemantauan kepatuhan.

Tautan produk

Dokumentasi mitra

Plérion – Platform Keamanan Cloud

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerionadalah Platform Keamanan Cloud dengan pendekatan berbasis ancaman unik yang didorong oleh risiko yang menawarkan tindakan pencegahan, detektif, dan korektif di seluruh beban kerja Anda. Integrasi antara Plerion dan Security Hub CSPM memungkinkan pelanggan untuk memusatkan dan bertindak berdasarkan temuan keamanan mereka di satu tempat.

AWS Tautan pasar

Dokumentasi mitra

Penjelajah – Penjelajah

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowleradalah alat keamanan open source untuk melakukan AWS pemeriksaan terkait praktik terbaik keamanan, pengerasan, dan pemantauan berkelanjutan.

Tautan produk

Dokumentasi mitra

Qualys – Manajemen Kerentanan

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)terus memindai dan mengidentifikasi kerentanan, melindungi aset Anda.

Tautan produk

Dokumentasi mitra

Cepat7 – InsightVM

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVMmenyediakan manajemen kerentanan untuk lingkungan modern, memungkinkan Anda menemukan, memprioritaskan, dan memperbaiki kerentanan secara efisien.

Tautan produk

Dokumentasi mitra

SentinelOne – SentinelOne

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOneadalah platform deteksi dan respons yang diperluas (XDR) otonom yang mencakup AI-powered pencegahan, deteksi, respons, dan perburuan di seluruh titik akhir, wadah, beban kerja cloud, dan perangkat IoT.

AWS Tautan pasar

Tautan produk

Snyk

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snykmenyediakan platform keamanan yang memindai komponen aplikasi untuk risiko keamanan dalam beban kerja yang berjalan AWS. Risiko ini dikirim ke Security Hub CSPM sebagai temuan,

membantu pengembang dan tim keamanan memvisualisasikan dan memprioritaskannya bersama dengan temuan AWS keamanan lainnya.

AWS Tautan pasar

Dokumentasi mitra

Keamanan Sonrai – Sonrai Dig

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Digmemantau dan memperbaiki kesalahan konfigurasi cloud dan pelanggaran kebijakan, sehingga Anda dapat meningkatkan postur keamanan dan kepatuhan Anda.

Tautan produk

Dokumentasi mitra

Sophos – Perlindungan Server

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protectionmembela aplikasi dan data penting di inti organisasi Anda, menggunakan teknik pertahanan mendalam yang komprehensif.

Tautan produk

StackRox – StackRox Keamanan Kubernetes

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRoxmembantu perusahaan mengamankan penyebaran container dan Kubernetes mereka dalam skala besar dengan menegakkan kebijakan kepatuhan dan keamanan mereka di seluruh siklus hidup kontainer — membangun, menerapkan, dan menjalankan.

Tautan produk

Dokumentasi mitra

Logika Sumo – Analisis Data Mesin

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logicadalah platform analisis data mesin yang aman yang memungkinkan tim operasi pengembangan dan keamanan untuk membangun, menjalankan, dan mengamankan AWS aplikasi mereka.

Tautan produk

Dokumentasi mitra

Symantec – Perlindungan Beban Kerja Cloud

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protectionmemberikan perlindungan lengkap untuk instans Amazon EC2 Anda dengan antimalware, pencegahan intrusi, dan pemantauan integritas file.

Tautan produk

Dokumentasi mitra

Dapat dipertahankan – Tenable.io

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Secara akurat mengidentifikasi, menyelidiki, dan memprioritaskan kerentanan. Dikelola di cloud.

Tautan produk

Dokumentasi mitra

Trend Micro – Awan Satu

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud Onememberikan informasi keamanan yang tepat kepada tim pada waktu dan tempat yang tepat. Integrasi ini mengirimkan temuan keamanan ke Security Hub CSPM secara real time, meningkatkan visibilitas ke AWS sumber daya dan detail Trend Micro Cloud One acara Anda di Security Hub CSPM.

AWS Tautan pasar

Dokumentasi mitra

Vectra – Deteksi Cognito

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectramengubah keamanan siber dengan menerapkan AI canggih untuk mendeteksi dan menanggapi penyerang siber tersembunyi sebelum mereka dapat mencuri atau menyebabkan kerusakan.

AWS Tautan pasar

Dokumentasi mitra

Wiz – Keamanan Wiz

Jenis integrasi: Kirim

Produk ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wizterus menganalisis konfigurasi, kerentanan, jaringan, pengaturan IAM, rahasia, dan lainnya di seluruh Anda Akun AWS, pengguna, dan beban kerja untuk menemukan masalah kritis yang mewakili risiko aktual. Integrasikan Wiz dengan Security Hub CSPM untuk memvisualisasikan dan menanggapi masalah yang dideteksi Wiz dari konsol CSPM Security Hub.

AWS Tautan pasar

Dokumentasi mitra

Third-party integrasi yang menerima temuan dari Security Hub CSPM

Integrasi produk mitra pihak ketiga berikut dapat menerima temuan dari Security Hub CSPM. Jika dicatat, produk mungkin juga memperbarui temuan. Dalam hal ini, pembaruan yang Anda buat untuk temuan dalam produk mitra juga tercermin dalam Security Hub CSPM.

Atlassian - Manajemen Layanan Jira

Jenis integrasi: Terima dan perbarui

AWS Service Management Connector Untuk Jira mengirimkan temuan dari Security Hub CSPM ke. Jira Jiramasalah dibuat berdasarkan temuan. Saat Jira masalah diperbarui, temuan terkait diperbarui di Security Hub CSPM.

Integrasi hanya mendukung Jira Server dan Jira Data Center.

Untuk ikhtisar integrasi dan cara kerjanya, tonton video AWS Security Hub CSPM — Integrasi dua arah dengan. Atlassian Jira Service Management

Tautan produk

Dokumentasi mitra

Atlassian - Cloud Manajemen Layanan Jira

Jenis integrasi: Terima dan perbarui

Jira Service Management Cloudadalah komponen cloud dari Jira Service Management.

AWS Service Management Connector Untuk Jira mengirimkan temuan dari Security Hub CSPM ke. Jira Temuan ini memicu terciptanya masalah diJira Service Management Cloud. Saat Anda memperbarui masalah tersebutJira Service Management Cloud, temuan terkait juga diperbarui di Security Hub CSPM.

Tautan produk

Dokumentasi mitra

Atlassian – Opsgenie

Jenis integrasi: Terima

Opsgenieadalah solusi manajemen insiden modern untuk mengoperasikan layanan yang selalu aktif, memberdayakan tim pengembangan dan operasi untuk merencanakan gangguan layanan dan tetap memegang kendali selama insiden.

Mengintegrasikan dengan Security Hub CSPM memastikan bahwa insiden terkait keamanan misi kritis diarahkan ke tim yang sesuai untuk penyelesaian segera.

Tautan produk

Dokumentasi mitra

Dynatrace

Jenis integrasi: Terima

DynatraceIntegrasi dengan Security Hub CSPM membantu menyatukan, memvisualisasikan, dan mengotomatiskan temuan keamanan di seluruh alat dan lingkungan. Men Dynatrace ambahkan konteks runtime ke temuan keamanan memungkinkan prioritas yang lebih cerdas, membantu mengurangi kebisingan dari peringatan, dan memfokuskan DevSecOps tim Anda untuk memperbaiki masalah kritis yang memengaruhi lingkungan produksi dan aplikasi Anda secara efisien.

Tautan produk

Dokumentasi mitra

Elastis

Jenis integrasi: Terima

Elasticmembangun solusi berbasis pencarian untuk keamanan, pengamatan, dan pencarian. Dengan integrasi Security Hub CSPM, Elastic menyerap temuan dan wawasan dari Security Hub CSPM secara terprogram, menormalkannya untuk korelasi dan analitik, dan menyajikan dasbor dan deteksi terpadu, memungkinkan triase dan investigasi yang lebih cepat tanpa menggunakan agenElastic Security.

Tautan produk

Dokumentasi mitra

Fortinet – ForticNP

Jenis integrasi: Terima

FortiCNPadalah produk Cloud Native Protection yang menggabungkan temuan keamanan menjadi wawasan yang dapat ditindaklanjuti dan memprioritaskan wawasan keamanan berdasarkan skor risiko untuk mengurangi kelelahan peringatan dan mempercepat remediasi.

AWS Tautan pasar

Dokumentasi mitra

IBM – QRadar

Jenis integrasi: Terima

IBM QRadarSIEM menyediakan tim keamanan dengan kemampuan untuk mendeteksi, memprioritaskan, menyelidiki, dan menanggapi ancaman dengan cepat dan akurat.

Tautan produk

Dokumentasi mitra

Logz.io Awan SIEM

Jenis integrasi: Terima

Logz.ioadalah penyedia Cloud SIEM yang menyediakan korelasi lanjutan dari log dan data peristiwa untuk membantu tim keamanan mendeteksi, menganalisis, dan menanggapi ancaman keamanan secara real time.

Tautan produk

Dokumentasi mitra

MetricStream – CyberGRC

Jenis integrasi: Terima

MetricStream CyberGRCmembantu Anda mengelola, mengukur, dan mengurangi risiko keamanan siber. Dengan menerima temuan Security Hub CSPM, CyberGRC memberikan visibilitas yang lebih besar ke dalam risiko ini, sehingga Anda dapat memprioritaskan investasi keamanan siber dan mematuhi kebijakan TI.

AWS Tautan pasar

Tautan produk

MicroFocus – MicroFocus Arcsight

Jenis integrasi: Terima

ArcSightmempercepat deteksi dan respons ancaman yang efektif secara real time, mengintegrasikan korelasi peristiwa dan analitik yang diawasi dan tidak diawasi dengan otomatisasi dan orkestrasi respons.

Tautan produk

Dokumentasi mitra

Manajemen Kerentanan Peninggalan Baru

Jenis integrasi: Terima

New Relic Vulnerability Managementmenerima temuan keamanan dari Security Hub CSPM, sehingga Anda bisa mendapatkan tampilan keamanan terpusat bersama telemetri kinerja dalam konteks di seluruh stack Anda.

AWS Tautan pasar

Dokumentasi mitra

PagerDuty – PagerDuty

Jenis integrasi: Terima

Platform manajemen operasi PagerDuty digital memberdayakan tim untuk secara proaktif mengurangi masalah yang berdampak pada pelanggan dengan secara otomatis mengubah sinyal apa pun menjadi wawasan dan tindakan yang tepat.

AWS pengguna dapat menggunakan PagerDuty serangkaian AWS integrasi untuk menskalakan lingkungan mereka AWS dan hibrida dengan percaya diri.

Ketika digabungkan dengan peringatan keamanan yang dikumpulkan dan terorganisir di Security Hub CSPM, PagerDuty memungkinkan tim untuk mengotomatiskan proses respons ancaman mereka dan dengan cepat mengatur tindakan khusus untuk mencegah potensi masalah.

PagerDutypengguna yang melakukan proyek migrasi cloud dapat bergerak cepat, sekaligus mengurangi dampak masalah yang terjadi sepanjang siklus migrasi.

Tautan produk

Dokumentasi mitra

Jaringan Palo Alto – Korteks XSOAR

Jenis integrasi: Terima

Cortex XSOARadalah platform Security Orchestration, Automation, and Response (SOAR) yang terintegrasi dengan seluruh tumpukan produk keamanan Anda untuk mempercepat respons insiden dan operasi keamanan.

Tautan produk

Dokumentasi mitra

Jaringan Palo Alto – VM-Series

Jenis integrasi: Terima

Palo Alto VM-Seriesintegrasi dengan Security Hub CSPM mengumpulkan intelijen ancaman dan mengirimkannya ke firewall VM-Series generasi berikutnya sebagai pembaruan kebijakan keamanan otomatis yang memblokir aktivitas alamat IP berbahaya.

Tautan produk

Dokumentasi mitra

Teknologi Rackspace – Keamanan Asli Cloud

Jenis integrasi: Terima

Rackspace Technology menyediakan layanan keamanan terkelola di atas produk AWS keamanan asli untuk pemantauan 24x7x365 oleh Rackspace SOC, analisis lanjutan, dan remediasi ancaman.

Tautan produk

Cepat7 – InsightConnect

Jenis integrasi: Terima

Rapid7 InsightConnectadalah solusi orkestrasi keamanan dan otomatisasi yang memungkinkan tim Anda mengoptimalkan operasi SOC dengan sedikit atau tanpa kode.

Tautan produk

Dokumentasi mitra

RSA – Pemanah RSA

Jenis integrasi: Terima

RSA ArcherManajemen Risiko TI dan Keamanan memungkinkan Anda menentukan aset mana yang penting bagi bisnis Anda, menetapkan dan mengkomunikasikan kebijakan dan standar keamanan, mendeteksi dan menanggapi serangan, mengidentifikasi dan memperbaiki kekurangan keamanan, dan menetapkan praktik terbaik manajemen risiko TI yang jelas.

Tautan produk

Dokumentasi mitra

ServiceNow – ITSM

Jenis integrasi: Terima dan perbarui

ServiceNowIntegrasi dengan Security Hub CSPM memungkinkan temuan keamanan dari Security Hub CSPM untuk dilihat di dalam. ServiceNow ITSM Anda juga dapat mengonfigurasi ServiceNow untuk secara otomatis membuat insiden atau masalah saat menerima temuan dari Security Hub CSPM.

Setiap pembaruan untuk insiden dan masalah ini menghasilkan pembaruan pada temuan di Security Hub CSPM.

Untuk ikhtisar integrasi dan cara kerjanya, tonton video AWS Security Hub CSPM - Integrasi dua arah dengan. ServiceNow ITSM

Tautan produk

Dokumentasi mitra

Slack – Slack

Jenis integrasi: Terima

Slackadalah lapisan tumpukan teknologi bisnis yang menyatukan orang, data, dan aplikasi. Ini adalah satu tempat di mana orang dapat bekerja sama secara efektif, menemukan informasi penting, dan mengakses ratusan ribu aplikasi dan layanan penting untuk melakukan pekerjaan terbaik mereka.

Tautan produk

Dokumentasi mitra

Splunk – Perusahaan Splunk

Jenis integrasi: Terima

Splunkmenggunakan Amazon CloudWatch Events sebagai konsumen temuan Security Hub CSPM. Kirim data Anda ke Splunk untuk analisis keamanan lanjutan dan SIEM.

Tautan produk

Dokumentasi mitra

Splunk – Phantom Splunk

Jenis integrasi: Terima

Dengan Splunk Phantom aplikasi untuk AWS Security Hub CSPM, temuan dikirim ke Phantom untuk pengayaan konteks otomatis dengan informasi intelijen ancaman tambahan atau untuk melakukan tindakan respons otomatis.

Tautan produk

Dokumentasi mitra

ThreatModeler

Jenis integrasi: Terima

ThreatModeleradalah solusi pemodelan ancaman otomatis yang mengamankan dan menskalakan siklus hidup pengembangan perangkat lunak perusahaan dan cloud.

Tautan produk

Dokumentasi mitra

Trelliks – Trellix Helix

Jenis integrasi: Terima

Trellix Helixadalah platform operasi keamanan yang di-host cloud yang memungkinkan organisasi untuk mengendalikan setiap insiden dari peringatan hingga perbaikan.

Tautan produk

Dokumentasi mitra

Third-party integrasi yang mengirimkan temuan ke dan menerima temuan dari Security Hub CSPM

Integrasi produk mitra pihak ketiga berikut dapat mengirimkan temuan ke dan menerima temuan dari Security Hub CSPM.

Caveonix – Awan Caveonix

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Caveonix AI-powered Platform ini mengotomatiskan visibilitas, penilaian, dan mitigasi di cloud hybrid, mencakup layanan cloud-native, VM, dan container. Terintegrasi dengan AWS Security Hub CSPM, Caveonix menggabungkan AWS data dan analitik lanjutan untuk wawasan tentang peringatan keamanan dan kepatuhan.

AWS Tautan pasar

Dokumentasi mitra

Kustodian Cloud – Kustodian Cloud

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodianmemungkinkan pengguna untuk dikelola dengan baik di cloud. YAML DSL sederhana memungkinkan aturan yang mudah ditentukan untuk mengaktifkan infrastruktur cloud yang dikelola dengan baik yang aman dan dioptimalkan biaya.

Tautan produk

Dokumentasi mitra

DisruptOps, Inc. – DisrupTop

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

Platform Operasi DisruptOps Keamanan membantu organisasi mempertahankan praktik keamanan terbaik di cloud Anda melalui penggunaan pagar pembatas otomatis.

Tautan produk

Dokumentasi mitra

Kion

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(sebelumnya cloudtamer.io) adalah solusi tata kelola cloud lengkap untuk. AWSKionmemberikan visibilitas pemangku kepentingan ke dalam operasi cloud dan membantu pengguna cloud mengelola akun, mengontrol anggaran dan biaya, serta memastikan kepatuhan berkelanjutan.

Tautan produk

Dokumentasi mitra

Turbot – Turbot

Jenis integrasi: Kirim dan terima

Produk ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbotmemastikan bahwa infrastruktur cloud Anda aman, sesuai, dapat diskalakan, dan dioptimalkan biaya.

Tautan produk

Dokumentasi mitra

Mengintegrasikan Security Hub CSPM dengan produk khusus

Selain temuan yang dihasilkan oleh AWS layanan terintegrasi dan produk pihak ketiga, AWS Security Hub CSPM dapat menggunakan temuan yang dihasilkan oleh produk keamanan khusus lainnya.

Anda dapat mengirim temuan ini ke Security Hub CSPM dengan menggunakan pen BatchImportFindings goperasian Security Hub CSPM API. Anda dapat menggunakan operasi yang sama untuk memperbarui temuan dari produk kustom yang sudah Anda kirim ke Security Hub CSPM.

Saat menyiapkan integrasi kustom, gunakan pedoman dan daftar periksa yang disediakan di Panduan Integrasi Mitra CSPM Hub Keamanan.

Persyaratan dan rekomendasi untuk integrasi produk khusus

Sebelum Anda berhasil memanggil operasi `BatchImportFindings` API, Anda harus mengaktifkan Security Hub CSPM.

Anda juga harus memberikan detail pencarian untuk produk khusus menggunakanthe section called "Format pencarian: ASFF". Tinjau persyaratan dan rekomendasi berikut untuk integrasi produk khusus:

Mengatur produk ARN

Saat Anda mengaktifkan Security Hub CSPM, produk default Amazon Resource Name (ARN) untuk Security Hub CSPM akan dibuat di akun Anda saat ini.

Produk ARN ini memiliki format sebagai berikut:`arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`. Misalnya, `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

Gunakan ARN produk ini sebagai nilai `ProductArn` atribut saat memanggil operasi `BatchImportFindings` API.

Menetapkan nama perusahaan dan produk

Anda dapat menggunakan `BatchImportFindings` untuk menetapkan nama perusahaan dan nama produk pilihan untuk integrasi kustom yang mengirimkan temuan ke Security Hub CSPM.

Nama yang Anda tentukan menggantikan nama perusahaan dan nama produk yang telah dikonfigurasi sebelumnya, masing-masing disebut nama pribadi dan nama default, dan muncul di konsol CSPM Hub Keamanan dan JSON dari setiap temuan. Lihat BatchImportFindings untuk menemukan penyedia.

Mengatur ID temuan

Anda harus menyediakan, mengelola, dan menambah ID temuan Anda sendiri, menggunakan `Id` atribut.

Setiap temuan baru harus memiliki ID temuan yang unik. Jika produk kustom mengirimkan beberapa temuan dengan ID temuan yang sama, Security Hub CSPM hanya memproses temuan pertama.

Mengatur ID akun

Anda harus menentukan ID akun Anda sendiri, menggunakan `AwsAccountId` atribut.

Mengatur yang dibuat pada dan diperbarui pada tanggal

Anda harus memberikan stempel waktu Anda sendiri untuk atribut `CreatedAt` dan `UpdatedAt`.

Memperbarui temuan dari produk khusus

Selain mengirimkan temuan baru dari produk khusus, Anda juga dapat menggunakan operasi `BatchImportFindings` API untuk memperbarui temuan yang ada dari produk khusus.

Untuk memperbarui temuan yang ada, gunakan ID temuan yang ada (melalui `Id` atribut). Kirim ulang temuan lengkap dengan informasi yang sesuai diperbarui dalam permintaan, termasuk stempel waktu yang dimodifikasi `UpdatedAt`.

Contoh integrasi kustom

Anda dapat menggunakan contoh integrasi produk kustom berikut sebagai panduan untuk membuat solusi kustom Anda sendiri:

Mengirim temuan dari Chef InSpec pemindaian ke Security Hub CSPM

Anda dapat membuat CloudFormation template yang menjalankan pemindaian Chef InSpec kepatuhan dan kemudian mengirimkan temuan ke Security Hub CSPM.

Untuk detail selengkapnya, lihat Pemantauan kepatuhan berkelanjutan dengan Chef InSpec dan AWS Security Hub CSPM.

Mengirim kerentanan wadah yang terdeteksi oleh Trivy ke Security Hub CSPM

Anda dapat membuat CloudFormation template yang digunakan AquaSecurity Trivy untuk memindai wadah untuk kerentanan, dan kemudian mengirimkan temuan kerentanan tersebut ke Security Hub CSPM.

Untuk detail selengkapnya, lihat Cara membuat CI/CD pipeline untuk pemindaian kerentanan kontainer dengan Trivy dan AWS Security Hub CSPM.

Mengintegrasikan CSPM Security Hub dengan Microsoft Azure

Untuk memantau sumber daya Microsoft Azure, Anda dapat mengintegrasikan Microsoft Azure dengan AWS Security Hub CSPM. Security Hub CSPM kemudian secara otomatis mengaktifkan pemeriksaan manajemen postur untuk lingkungan Azure Anda dan menghasilkan temuan tentang lingkungan Anda. Lebih khusus lagi, layanan ini memberi Anda hal-hal berikut:

> **Note**
>
> Anda dapat mengelola standar dan kontrol Azure menggunakan konsol CSPM Security Hub, API, dan. AWS CloudFormation Fitur Security Hub CSPM Central Configuration tidak didukung untuk standar Azure.

- Temuan ASFF - Security Hub CSPM menghasilkan temuan dalam format AWS Security Finding Format (ASFF) untuk pemeriksaan postur yang dilakukan untuk sumber daya Azure Anda.
- CIS Microsoft Azure Foundations Benchmark v4.0 — Pemeriksaan kepatuhan otomatis terhadap standar CIS Azure v4.0. Standar ini mencakup identitas, jaringan, penyimpanan, logging, dan kontrol database.
- Azure Foundational Best Practices — Deteksi otomatis kesalahan konfigurasi sumber daya Azure berdasarkan praktik terbaik keamanan yang AWS dikuratori yang mencakup keamanan jaringan, manajemen identitas, perlindungan data, dan pencatatan.
- Manajemen postur - Evaluasi berkelanjutan konfigurasi sumber daya Azure terhadap praktik terbaik keamanan dan standar kepatuhan, dengan 122 kontrol di kedua standar.
- Per-provider skor keamanan — Pisahkan skor keamanan untuk AWS dan Azure, sehingga Anda dapat melacak setiap lingkungan secara mandiri.

Untuk membuat integrasi, Anda menghubungkan lingkungan Azure Anda ke Security Hub CSPM melalui proses berikut:

> **Note**
>
> Standar Azure berbeda dari AWS standar dengan cara berikut:
>
> - Standar Azure tidak memerlukan AWS Config prasyarat manual. Tidak seperti AWS, di mana CSPM-only pelanggan membutuhkan perekam terkelola pelanggan, standar Azure menggunakan perekam terkait layanan internal secara otomatis.

- Standar Azure selalu menggunakan aturan konfigurasi terkait layanan internal. AWS standar hanya menggunakan aturan konfigurasi terkait layanan saat Security Hub juga diaktifkan.

1. Anda mengonfigurasi lingkungan Azure Anda dengan pendaftaran aplikasi, kredenal identitas federasi, penetapan peran Azure, dan infrastruktur Event Hub.
2. Dengan menggunakan konsol CSPM Security Hub, Anda membuat konektor untuk integrasi. Anda menentukan ID penyewa Azure, ID klien aplikasi, dan cakupan pemantauan.
3. AWS Config mengumpulkan data konfigurasi sumber daya dari lingkungan Azure Anda.

   AWS Config digunakan secara internal untuk mengumpulkan data konfigurasi sumber daya. Tidak seperti manajemen AWS postur, di mana Anda harus secara eksplisit mengaktifkan AWS Config dan membayar untuk perekaman, manajemen postur Azure menangani secara otomatis. AWS Config Anda tidak perlu mengaktifkan AWS Config secara terpisah, mengonfigurasi perekam, atau membayar secara terpisah untuk AWS Config penggunaan. Biaya ini sudah termasuk dalam harga CSPM Security Hub Anda.
4. Security Hub CSPM mulai menerima data konfigurasi sumber daya dan peristiwa Log Aktivitas dari lingkungan Azure Anda.
5. Security Hub CSPM menghasilkan temuan manajemen postur tentang lingkungan Azure Anda.

Bagaimana AWS Config digunakan

AWS Config digunakan secara internal untuk mengumpulkan data konfigurasi sumber daya dan mendeteksi perubahan di lingkungan Azure Anda. Konektor menangani ini secara otomatis. Anda tidak perlu mengaktifkan AWS Config secara terpisah, mengkonfigurasi perekam, atau membayar untuk AWS Config penggunaan. Biaya ini sudah termasuk dalam harga CSPM Security Hub Anda untuk sumber daya Azure.

Service-linked konektor dan konektor yang dikelola pelanggan

Security Hub CSPM mendukung dua jenis konektor:

Service-linked konektor (SLC)

Dibuat secara otomatis saat Anda mengatur integrasi Azure di Security Hub. Cakupan konektor terkait layanan selalu cocok dengan cakupan yang ditentukan dalam konektor Security Hub

Anda. Anda tidak dapat memodifikasi cakupan konektor terkait layanan secara langsung; sebagai gantinya, ubah ruang lingkup di Security Hub. Security Hub mengelola siklus hidup konektor terkait layanan atas nama Anda.

Customer-managed konektor (CMC)

Dibuat langsung di konsol CSPM Security Hub di halaman Integrasi. Gunakan konektor yang dikelola pelanggan saat Anda ingin menggunakan Security Hub CSPM secara independen dari Security Hub, atau saat Anda memerlukan cakupan yang berbeda dari konektor Security Hub Anda. Ketika kedua jenis ada, cakupan konektor terkait layanan harus selalu sama atau lebih besar dari cakupan konektor yang dikelola pelanggan Anda.

> **Note**
>
> Tidak seperti Security Hub, Security Hub CSPM tidak menawarkan pilihan per kemampuan untuk konektor Azure. Saat Anda membuat konektor di Security Hub CSPM, semua kemampuan manajemen postur diaktifkan bersama-sama.

Untuk informasi tentang memperkirakan dan menghitung biaya untuk mengintegrasikan CSPM Security Hub dengan Azure, lihat harga CSPM Security Hub AWS .

Topik

- Prasyarat untuk mengintegrasikan Security Hub CSPM dengan Microsoft Azure
- Mengkonfigurasi Microsoft Azure untuk mengintegrasikan dengan Security Hub CSPM
- Mengkonfigurasi CSPM Security Hub untuk berintegrasi dengan Microsoft Azure
- Menghapus konektor Microsoft Azure di Security Hub CSPM

Prasyarat untuk mengintegrasikan Security Hub CSPM dengan Microsoft Azure

Sebelum Anda mengintegrasikan Microsoft Azure dengan AWS Security Hub CSPM, selesaikan tugas-tugas berikut di lingkungan Anda AWS dan Azure. Ini membantu memastikan bahwa Anda dan Security Hub CSPM memiliki sumber daya dan izin yang Anda perlukan untuk memantau sumber daya Azure Anda.

Topik

- Prasyarat untuk AWS
- Prasyarat untuk Microsoft Azure

Prasyarat untuk AWS

Verifikasi bahwa Anda memiliki yang berikut di Akun AWS:

AWS Security Hub CSPM diaktifkan

Security Hub CSPM harus diaktifkan di Akun AWS dan Wilayah AWS di mana Anda ingin membuat konektor.

Izin IAM konsol

Prinsipal IAM yang membuat konektor harus memiliki izin berikut:

- `config:GetConnector`
- `config:ListConnectors`
- `config:PutConnector`

Federasi Identitas Keluar IAM diaktifkan

Anda harus mengaktifkan IAM Outbound Identity Federation di. Akun AWS Fitur ini memungkinkan AWS layanan untuk mengautentikasi ke penyedia identitas eksternal (seperti Microsoft Entra ID) menggunakan kredensi federasi daripada rahasia berumur panjang.

Setelah mengaktifkan Federasi Identitas Keluar, perhatikan URL Penerbit Token. URL ini mengikuti format:

```
https://uuid.tokens.sts.global.api.aws
```

Anda akan memerlukan URL ini saat mengonfigurasi kredensi identitas federasi di Azure.

Prasyarat untuk Microsoft Azure

Verifikasi bahwa Anda memiliki yang berikut di lingkungan Azure Anda:

Penyewa Azure

Anda harus memiliki penyewa Azure di cloud komersial Azure. Pemerintah Azure dan Azure China tidak didukung.

Ketersediaan log ID Microsoft Entra

Rekaman sumber daya memerlukan log audit Microsoft Graph dan log masuk dari penyewa ID Microsoft Entra Anda. Beberapa log ID Microsoft Entra memerlukan lisensi Microsoft Entra ID P1 atau P2.

Jika penyewa tidak memiliki log yang diperlukan, perekaman sumber daya mungkin melaporkan kegagalan sebagian. Pendaftaran aplikasi dan penetapan peran Azure tidak menyediakan data log yang hilang.

Peran Administrator Global

Orang yang mengonfigurasi lingkungan Azure harus memiliki peran Administrator Global di Microsoft Entra ID. Peran ini diperlukan untuk mendaftarkan aplikasi, memberikan persetujuan admin untuk izin Microsoft Graph API, menetapkan peran RBAC di lingkup grup manajemen root penyewa, dan mengonfigurasi pengaturan diagnostik untuk Log Audit ID Entra.

> **Note**
>
> Di banyak organisasi, Administrator Global Azure dan administrator AWS keamanan adalah orang yang berbeda. Pengaturan Azure dapat diselesaikan secara independen menggunakan skrip pengaturan yang dihasilkan.

Pendaftaran aplikasi Azure

Anda harus mendaftarkan aplikasi di Microsoft Entra ID. Aplikasi ini berfungsi sebagai identitas yang AWS digunakan untuk mengautentikasi ke lingkungan Azure Anda menggunakan kredensi federasi. Tidak ada rahasia klien yang diperlukan.

Hub Acara Azure

Anda harus membuat namespace Azure Event Hub dan instance Event Hub untuk menerima peristiwa Log Aktivitas dan Log Audit Entra ID. Skrip pengaturan mengotomatiskan pembuatan ini.

Izin Microsoft Graph API

Aplikasi terdaftar memerlukan izin Microsoft Graph API berikut (Jenis aplikasi, memerlukan persetujuan admin):

- `Directory.Read.All`— Baca data direktori termasuk pengguna, grup, dan prinsip layanan.
- `AuditLog.Read.All`— Baca peristiwa log audit Entra ID.
- `Policy.Read.All`— Baca kebijakan organisasi dan konfigurasi akses bersyarat.

Peran Pembaca Azure RBAC

Prinsipal layanan harus diberi peran Pembaca di lingkup grup manajemen root penyewa. Ini memberikan akses hanya-baca ke semua sumber daya Azure di semua langganan di penyewa.

Setelah Anda menyelesaikan tugas-tugas ini, Anda siap untuk mengkonfigurasi lingkungan Azure Anda.

Mengkonfigurasi Microsoft Azure untuk mengintegrasikan dengan Security Hub CSPM

Setelah menyelesaikan tugas prasyarat, Anda dapat mengonfigurasi lingkungan Microsoft Azure Anda untuk mendukung integrasi dengan AWS Security Hub CSPM. Untuk membantu Anda melakukan hal ini, konsol CSPM Security Hub menghasilkan skrip penyiapan yang disesuaikan untuk konfigurasi Anda.

Untuk menghasilkan skrip, lakukan hal berikut:

1. Buka konsol CSPM Security Hub.
2. Di panel navigasi, pilih Integrasi.
3. Pilih Buat konektor Azure.
4. Lengkapi konfigurasi konektor (ID penyewa, ruang lingkup, dan nama), lalu salin skrip penyiapan yang dihasilkan.

Untuk menjalankan skrip, gunakan Azure CLI dan autentikasi dengan akun Administrator Global (`az login`).

Ketika Anda menjalankan skrip, ia melakukan serangkaian tugas. Bagian berikut menjelaskan setiap tugas yang dilakukan skrip. Jika organisasi Anda membatasi eksekusi skrip, Anda dapat melakukan tugas-tugas ini secara manual, menggunakan topik ini sebagai panduan. Setelah mengonfigurasi lingkungan Azure, Anda dapat mengonfigurasi Security Hub CSPM untuk diintegrasikan dengan Azure.

> **Note**
>
> Pendaftaran aplikasi Azure tunggal dibagikan di seluruh layanan AWS keamanan. Jika Anda juga menggunakan Security Hub atau Amazon Inspector untuk Azure, mereka menggunakan

pendaftaran aplikasi yang sama. Anda tidak perlu membuat pendaftaran terpisah untuk setiap AWS layanan.

Tugas

- Langkah 1: Daftarkan aplikasi Azure
- Langkah 2: Buat prinsipal layanan
- Langkah 3: Konfigurasikan kredentif identitas federasi
- Langkah 4: Tetapkan peran Pembaca
- Langkah 5: Konfigurasikan izin Microsoft Graph API
- Langkah 6: Siapkan Azure Event Hub
- Langkah 7: Konfigurasikan Log Aktivitas dan ekspor Log Audit ID Entra

Langkah 1: Daftarkan aplikasi Azure

Daftarkan aplikasi baru di Microsoft Entra ID. Aplikasi ini berfungsi sebagai identitas yang digunakan untuk men AWS gotentikasi ke lingkungan Azure Anda menggunakan kredenSIAL federasi. Tidak ada rahasia klien yang diperlukan.

```
$ az ad app create --display-name "AWSSecurityHubIntegration"
```

Perhatikan ID Aplikasi (klien) dari output (`appId`atribut). Anda akan memberikan nilai ini saat membuat konektor di konsol CSPM Hub Keamanan.

Langkah 2: Buat prinsipal layanan

Buat prinsip layanan untuk aplikasi terdaftar. Anda menggunakan penetapan peran Azure untuk memberikan izin kepada prinsipal layanan. Prinsip layanan melakukan tindakan di lingkungan Azure Anda.

```
$ az ad sp create --id application-client-id
```

Di *`application-client-id`* mana ID Aplikasi (klien) dari langkah sebelumnya.

Langkah 3: Konfigurasikan kredentif identitas federasi

Konfigurasikan kredentif identitas federasi pada aplikasi AWS untuk memungkinkan otentikasi tanpa rahasia klien. Ini menetapkan kepercayaan OIDC antara AWS dan Azure. Tidak ada rahasia atau kredenSIAL berumur panjang yang disimpan.

```
$ az ad app federated-credential create \
  --id application-client-id \
  --parameters '{
    "name": "AWSConfigFederation",
    "issuer": "token-issuer-url",
    "subject": "arn:aws:iam::account-id:role/aws-service-role/
thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty",
    "audiences": ["api://AzureADTokenExchange"],
    "description": "Federation for AWS Config third-party cloud resource discovery"
  }'
```

Nilai-nilai kunci:

- Penerbit — URL Penerbit Token Anda dari Federasi Identitas Keluar IAM. Ini mengikuti format`https://uuid.tokens.sts.global.api.aws`.
- Sub jek — ARN dari peran `AWSServiceRoleForConfigThirdParty` terkait layanan di Anda. Akun AWS AWS membuat peran terkait layanan ini secara otomatis selama pengaturan konektor.
- Audiens — `api://AzureADTokenExchange` (nilai standar untuk federasi identitas beban kerja).

Langkah 4: Tetapkan peran Pembaca

Tetapkan peran Pembaca ke prinsipal layanan di root scope (`/`). Ini memberikan akses baca-saja ke semua sumber daya Azure di semua langganan di penyewa.

> **⚠ Tetapkan Pembaca di cakupan root**
>
> Pastikan untuk menetapkan peran Pembaca di cakupan root (`/`), bukan lingkup grup manajemen root penyewa. Security Hub CSPM membaca sumber daya penetapan peran Azure di setiap lingkup, termasuk penugasan yang dicakup di root penyewa. Penugasan Pembaca di grup manajemen root tidak mencakup penugasan yang cakupannya`/`, jadi tanpanya pembacaan tersebut gagal dengan kesalahan otorisasi dan konektor dapat memasuki keadaan terdegradasi.

```
$ az role assignment create \
  --assignee application-client-id \
  --role "Reader" \
  --scope "/"
```

Root-scope penugasan membutuhkan akses yang lebih tinggi

Menetapkan peran di root scope (/) memerlukan akses yang ditingkatkan. Jika penetapan peran gagal, verifikasi bahwa manajemen akses untuk sumber daya Azure disetel ke Ya di Microsoft Entra ID > Properti. Kemudian keluar dan masuk kembali untuk menyegarkan token Anda.

Hapus elevasi akar sementara

Meng aktifkan manajemen Akses untuk sumber daya Azure memberikan administrator yang masuk peran Administrator Akses Pengguna di cakupan root (/), yang dapat mengelola akses di setiap grup langganan dan manajemen di penyewa. Setelah orientasi selesai, setel Manajemen akses untuk sumber daya Azure kembali ke Tidak di Microsoft Entra ID > Properti, simpan, dan keluar sehingga elevasi ini tidak tetap aktif.

Langkah 5: Konfigurasikan izin Microsoft Graph API

Berikan izin Microsoft Graph API berikut (jenis Aplikasi) ke aplikasi, lalu berikan persetujuan admin:

- `Application.Read.All`
- `AuditLog.Read.All`
- `DelegatedPermissionGrant.Read.All`
- `Device.Read.All`
- `Group.Read.All`
- `GroupMember.Read.All`
- `GroupSettings.Read.All`
- `Organization.Read.All`
- `Policy.Read.All`

- `RoleManagement.Read.Directory`
- `User.Read.All`
- `UserAuthenticationMethod.Read.All`

```
$ az ad app permission admin-consent --id application-client-id
```

Langkah 6: Siapkan Azure Event Hub

AWS Config menggunakan Azure Event Hub untuk menerima pemberitahuan hampir real-time tentang perubahan konfigurasi sumber daya di lingkungan Azure Anda. Skrip penyiapan membuat infrastruktur Event Hub dan menandainya untuk penemuan.

```
$ az group create \
  --name "aws-securityhub-integration" \
  --location event-hub-region

$ az eventhubs namespace create \
  --resource-group "aws-securityhub-integration" \
  --name "aws-securityhub-account-id" \
  --location event-hub-region \
  --sku Standard

$ az eventhubs eventhub create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --name "activitylog" \
  --message-retention 1 \
  --partition-count 4

$ az eventhubs eventhub consumer-group create \
  --resource-group "aws-securityhub-integration" \
  --namespace-name "aws-securityhub-account-id" \
  --eventhub-name "activitylog" \
  --name "AWSConfig"
```

Setelah membuat Event Hub, beri tag namespace untuk penemuan dan tetapkan peran Penerima Data:

```
$ az tag create \
```

```
  --resource-id namespace-resource-id \
  --tags "AWSConfig-account-id-region=activitylog"

$ az role assignment create \
  --assignee application-client-id \
  --role "Azure Event Hubs Data Receiver" \
  --scope namespace-resource-id
```

> **Note**
>
> Dalam format tag`AWSConfig-account-id-region`, *`account-id`* adalah Akun AWS ID 12 digit Anda dan *`region`* merupakan Wilayah AWS tempat Anda membuat konektor (misalnya,`us-east-1`). Nilai-nilai ini mengidentifikasi mana Akun AWS dan Wilayah yang memiliki integrasi Event Hub ini.

Konfigurasi kunci:

- Namespace SKU — Standar (diperlukan untuk kelompok konsumen).
- Nama Hub Acara `-activitylog`.
- Kelompok konsumen `-AWSConfig`.
- Tag - `AWSConfig-`*`account-id`*`-`*`region`* dengan nilai`activitylog`. Tag ini memungkinkan AWS Config untuk menemukan Event Hub secara otomatis.
- Penetapan peran — Penerima Data Hub Peristiwa Azure pada namespace.

Langkah 7: Konfigurasikan Log Aktivitas dan ekspor Log Audit ID Entra

Konfigurasikan Azure untuk mengekspor Log Aktivitas dan Log Audit ID Entra ke Event Hub.

Ekspor Log Aktivitas:

Konfigurasikan pengaturan diagnostik pada setiap langganan untuk mengekspor Log Aktivitas ke Hub Peristiwa. Skrip penyiapan mengonfigurasi ini secara otomatis untuk semua langganan yang dipantau. Log Aktivitas menangkap aktivitas tingkat langganan termasuk penetapan peran dan perubahan sumber daya.

Ekspor Log Audit ID Masuk:

Konfigurasikan pengaturan diagnostik pada Microsoft Entra ID untuk mengekspor log audit ke Event Hub yang sama. Arahkan ke Microsoft Entra ID > Pemantauan > Pengaturan diagnostik> Tambahkan pengaturan diagnostik. Aktif AuditLogs kan dan mengarahkan mereka ke Event Hub Anda.

Microsoft Defender untuk ekspor berkelanjutan Cloud (opsional):

Untuk meneruskan peringatan keamanan Defender for Cloud ke Security Hub CSPM, konfigurasikan ekspor berkelanjutan ke Event Hub Anda. Di portal Azure, arahkan ke Microsoft Defender for Cloud > Pengaturan lingkungan> pilih langganan > Ekspor berkelanjutan. Pilih Event Hub sebagai target ekspor dan pilih namespace Event Hub Anda. Akti fkan peringatan keamanan sebagai tipe data ekspor.

Konfigurasi acara data Amazon Inspector (opsional):

Jika Anda berencana menggunakan Amazon Inspector untuk pemindaian VM Azure, konfigurasi peristiwa data tambahan diperlukan. Untuk detail tentang mengonfigurasi peristiwa Inspector-specific data, lihat dokumentasi Amazon Inspector untuk integrasi Azure.

Mengkonfigurasi CSPM Security Hub untuk berintegrasi dengan Microsoft Azure

Setelah menyelesaikan tugas prasyarat dan mengonfigurasi lingkungan Microsoft Azure, Anda dapat mengonfigurasi CSPM Security Hub untuk AWS diintegrasikan dengan Azure. Untuk mengonfigurasi CSPM Security Hub agar terintegrasi dengan Azure, Anda membuat konektor. Setelah Anda membuat konektor, peristiwa berikut terjadi:

1. Security Hub CSPM memvalidasi kredensi Azure dan konektivitas ke lingkungan Azure Anda. Proses ini dapat memakan waktu beberapa menit.
2. AWS Config mulai menemukan dan merekam data konfigurasi untuk sumber daya Azure Anda.
3. Security Hub CSPM mulai menghasilkan temuan manajemen postur untuk sumber daya Azure Anda setelah pengumpulan data sumber daya selesai.

> **Note**
>
> Jika Anda sudah membuat konektor di Security Hub, konektor terkait layanan secara otomatis dibuat di Security Hub CSPM. Anda tidak perlu membuat konektor terpisah yang dikelola pelanggan kecuali Anda memerlukan cakupan yang berbeda.

Topik

- Buat konektor Azure
- Mengaktifkan standar dan kontrol
- Sesuaikan ruang lingkup konektor Azure
- Verifikasi kesehatan konektor Azure
- Memecahkan masalah konektor Azure
- Bagaimana Security Hub CSPM menangani pengidentifikasi sumber daya
- Kontrol yang tersedia untuk Azure

Buat konektor Azure

Untuk membuat konektor Microsoft Azure untuk lingkungan Anda, selesaikan langkah-langkah berikut dengan menggunakan konsol CSPM AWS Security Hub atau API.

1. Buka konsol CSPM Security Hub.
2. Di panel navigasi, pilih Integrasi.
3. Pilih Buat konektor Azure.
4. Untuk Azure Tenant ID, masukkan pengenal penyewa Azure Active Directory Anda.
5. Untuk Aplikasi (ID klien), masukkan ID aplikasi untuk pendaftaran aplikasi Azure yang Anda buat.
6. Konfigurasikan pengaturan tambahan dan ruang lingkup konektor dengan melakukan hal berikut:

    - Untuk Nama, masukkan nama unik untuk konektor. Nama dapat berisi hingga 50 karakter alfanumerik dan dapat mencakup tanda hubung (-).

      > **Important**
      >
      > Nama dan deskripsi digunakan untuk mengidentifikasi konten Anda, dan kami menyarankan Anda untuk tidak memasukkan informasi sensitif, rahasia, atau identitas pribadi (PII) di dalamnya.

    - Untuk Deskripsi, secara opsional masukkan deskripsi singkat tentang konektor. Deskripsi dapat berisi hingga 200 karakter.
    - Untuk Langganan, pilih Semua langganan untuk memantau semua langganan saat ini dan masa depan di penyewa, atau Langganan khusus untuk memantau hanya langganan yang

Anda tentukan. Jika Anda memilih untuk memantau hanya langganan tertentu, masukkan ID untuk masing-masing langganan.

- Untuk Wilayah, pilih wilayah Azure tempat sumber daya Anda digunakan.

> **Note**
>
> Kontrol yang mengevaluasi ID Microsoft Entra dan sumber daya Microsoft Graph memerlukan cakupan wilayah global untuk disertakan dalam konfigurasi integrasi Anda. Jika Anda memilih Wilayah Azure tertentu saja, kontrol ini tidak akan menghasilkan temuan.

7. Tinjau konfigurasi Anda dan pilih Buat konektor.

Setelah Anda membuat konektor, Security Hub CSPM memvalidasi kredensi Azure Anda dan memulai penemuan sumber daya. Konektor harus menunjukkan status Aktif dalam 2-5 menit.

Mengaktifkan standar dan kontrol

Setelah membuat konektor, Anda harus mengaktifkan standar keamanan Azure untuk mulai menghasilkan temuan. Untuk informasi umum tentang mengaktifkan standar dan mengelola kontrol, lihat Mengaktifkan standar dan Mengaktifkan dan menonaktifkan kontrol.

Standar yang tersedia

- CIS Microsoft Azure Foundations Benchmark v4.0 - Tolok ukur keamanan yang diadopsi secara luas yang mendefinisikan praktik terbaik untuk mengamankan lingkungan Azure. Setiap kontrol mengevaluasi aspek tertentu dari konfigurasi Azure Anda (misalnya, enkripsi akun penyimpanan, aturan grup keamanan jaringan, identitas, dan pengaturan akses).
- Azure Foundational Best Practices - Mengevaluasi sumber daya Azure untuk risiko eksposur dengan menghubungkan jangkauan jaringan, akses publik, dan indikator data sensitif. Menghasilkan temuan tipe paparan yang menyoroti sumber daya dengan risiko tinggi.

Standar Azure memiliki seperangkat kontrol mereka sendiri, terpisah dari AWS kontrol. Tidak ada kontrol lintas-cloud yang mengevaluasi keduanya AWS dan sumber daya Azure dalam satu pemeriksaan.

Mengaktifkan standar

Anda dapat mengaktifkan standar Azure melalui konsol CSPM Security Hub atau melalui. API/ CLI Arahkan ke Standar di konsol CSPM Security Hub dan aktifkan standar yang diinginkan. Atau, gunakan CLI:

```
$ aws securityhub batch-enable-standards \
  --standards-subscription-requests '[{"StandardsArn": "Standard-ARN"}]' \
  --region your-aws-region
```

> **Note**
>
> Anda dapat mengaktifkan standar Azure sebelum atau sesudah membuat konektor - mereka tidak digabungkan. Namun, temuan hanya akan dihasilkan setelah konektor dan standar aktif dan data sumber daya telah dikumpulkan.

Mengelola kontrol individu

Setelah standar diaktifkan (biasanya dalam hitungan detik), Anda dapat melihat dan mengelola kontrol individual:

- Lihat kontrol: Gunakan konsol CSPM Security Hub (Standards > select standard> Controls) atau API. `list-standards-control-associations`
- Nonaktifkan kontrol: Jika kontrol tertentu tidak berlaku untuk lingkungan Anda, Anda dapat menonaktifkannya.
- Konfigurasikan parameter khusus: Beberapa kontrol menerima parameter input khusus (misalnya, ambang batas panjang kata sandi). Ini dapat dikonfigurasi melalui `update-security-control` API.

Catatan penting

- Standar Azure berlaku secara seragam di seluruh cakupan konektor Anda. Anda tidak dapat mengaktifkan standar atau kontrol yang berbeda untuk langganan Azure yang berbeda dalam konektor yang sama.
- Kontrol bergantung pada ketersediaan data sumber daya. Setiap kontrol mengevaluasi jenis sumber daya Azure tertentu. Jika AWS Config belum mengumpulkan data konfigurasi untuk

jenis sumber daya tertentu, kontrol akan menghasilkan temuan PASS default untuk sumber daya tersebut. Temuan PASS default ini akan secara otomatis diperbarui ke evaluasi yang akurat saat data sumber daya tiba. Jangan memperlakukan skor kepatuhan awal sebagai akurat sampai pengumpulan data sumber daya selesai.

- Parameter input khusus untuk kontrol keamanan dapat dikonfigurasi bahkan sebelum membuat konektor - mereka bertahan secara independen.
- Kontrol yang mengevaluasi pengaturan tingkat langganan (misalnya, paket Microsoft Defender, peringatan log aktivitas) menghasilkan satu temuan per langganan Azure, bukan per sumber daya individu.
- Standar multicloud tidak dapat dimasukkan dalam kebijakan Konfigurasi Pusat. Anda harus mengelola pemberdayaan standar Azure secara independen di masing-masing Akun AWS dan. Wilayah AWS

Sesuaikan ruang lingkup konektor Azure

Setelah Anda membuat konektor Microsoft Azure, Anda dapat menyesuaikan cakupan konektor dengan mengubah Langganan Azure atau Wilayah Azure yang diponitor. Jika Anda menyesuaikan ruang lingkup, sebagian besar jenis perubahan akan berlaku dalam waktu sekitar 15 menit.

Sebelum Anda menyesuaikan ruang lingkup, perhatikan hal berikut:

- Cakupan konektor yang dikelola pelanggan tidak dapat melebihi cakupan konektor terkait layanan yang ada di akun dan Wilayah yang sama.
- Ketika Anda memperluas cakupan, Security Hub CSPM mulai menghasilkan temuan untuk sumber daya baru setelah AWS Config mengumpulkan data konfigurasi mereka.
- Saat Anda mengurangi ruang lingkup, temuan yang ada untuk sumber daya yang dihapus beralih ke status yang diarsipkan.

Verifikasi kesehatan konektor Azure

Anda dapat memeriksa kesehatan konektor Microsoft Azure kapan saja. Arahkan ke Integrasi di konsol CSPM Security Hub dan konfirmasikan konektor Anda menunjukkan status Aktif.

Temuan awal biasanya muncul dalam 15-30 menit setelah pengumpulan data sumber daya selesai.

> **Note**
>
> Status kesehatan konektor pada akhirnya konsisten. Ketika masalah izin atau konfigurasi terjadi, status konektor berubah menjadi Terdegradasi dengan cepat dengan pesan yang dapat ditindaklanjuti. Namun, setelah Anda memperbaiki masalah, status dapat memakan waktu hingga 24 jam untuk kembali ke Terhubung.
>
> - Status terdegradasi setelah perbaikan baru-baru ini tidak selalu menunjukkan masalah yang sedang berlangsung.
> - Untuk visibilitas real-time ke kegagalan perekaman, periksa CloudWatch metrik di namespace.

Memecahkan masalah konektor Azure

Jika Anda mengalami masalah dengan konektor Anda, gunakan informasi berikut untuk mendiagnosis dan menyelesaikan masalah umum.

Status konektor tidak sehat

Masalah ini biasanya terjadi jika kredensil federasi tidak dikonfigurasi dengan benar di Azure.

Untuk mengatasi masalah ini, verifikasi bahwa URL penerbit token dan subjek ARN di kredensi federasi Azure Anda cocok dengan Anda. Akun AWS

Tidak ada temuan setelah 30 menit

Masalah ini dapat terjadi jika Event Hub tidak menerima Log Aktivitas atau jika tidak ada standar yang diaktifkan.

Untuk mengatasi masalah ini, verifikasi bahwa namespace Event Hub ditandai dengan benar (`AWSConfig-`*`account-id`*`-`*`region`*`=activitylog`), grup `AWSConfig` konsumen ada, peran Penerima Data ditetapkan, dan setidaknya satu standar Azure diaktifkan.

Tidak dapat merekam beberapa sumber daya Azure

Kesalahan dapat terjadi karena salah satu alasan berikut:

- Lingkungan Azure tidak memenuhi prasyarat untuk perekaman sumber daya.
- Pendaftaran aplikasi tidak memiliki persetujuan admin untuk izin Microsoft Graph API.

- Tugas peran Pembaca tidak mencakup semua cakupan yang diperlukan.
- Penyewa ID Microsoft Entra tidak memiliki data log yang diperlukan.

Untuk mengatasi kesalahan, lakukan hal berikut:

1. Untuk mengonfirmasi bahwa lingkungan Anda memenuhi semua persyaratan, tinjau Prasyarat untuk Microsoft Azure.
2. Konfirmasikan bahwa pendaftaran aplikasi memiliki izin Microsoft Graph API yang diperlukan dengan persetujuan admin.
3. Verifikasi bahwa kepala layanan memiliki peran Pembaca di lingkup grup manajemen root penyewa.

Konektor tetap dalam status Tertunda

Masalah ini dapat terjadi jika pendaftaran aplikasi Azure salah dikonfigurasi.

Untuk mengatasi masalah ini, verifikasi bahwa URL penerbit kredensi identitas federasi dan pengenal subjek cocok dengan Anda. Akun AWS Juga verifikasi bahwa persetujuan admin telah diberikan untuk semua izin Microsoft Graph API yang diperlukan.

Bagaimana Security Hub CSPM menangani pengidentifikasi sumber daya

Dengan mengaktifkan integrasi Azure Anda untuk AWS Security Hub CSPM, pengidentifikasi sumber daya dari penyedia cloud lain akan disimpan di, Security AWS Config Hub AWS CSPM, dan AWS layanan lainnya (sesuai kebutuhan) sebagai metadata yang terkait dengan pengelolaan data konfigurasi sumber daya terkait yang dikumpulkan dari penyedia cloud lainnya. Pengidentifikasi sumber daya tersebut bukan merupakan Konten Anda, dan kami menyarankan Anda untuk tidak memasukkan informasi sensitif, rahasia, atau identitas pribadi di dalamnya.

Pengidentifikasi berikut dari lingkungan cloud Anda yang terhubung disimpan dan digunakan oleh AWS untuk menyediakan kemampuan keamanan multicloud:

- Pengidentifikasi sumber daya: ID Penyewa Azure, ID Langganan, Lokasi (wilayah), ID Sumber Daya (ID atau Nama Grup Sumber Daya, Penyedia Sumber Daya, Jenis Sumber Daya)

Hubungan antara pengidentifikasi ini - termasuk bagaimana sumber daya berhubungan satu sama lain dan bagaimana temuan berhubungan dengan sumber daya - juga disimpan sebagai metadata layanan. AWS menggunakan pengidentifikasi ini untuk korelasi sumber daya, mengaitkan temuan dengan sumber daya, pencatatan operasional layanan, dan de-duplikasi.

Kontrol yang tersedia untuk Azure

Setelah Anda mengaktifkan standar Azure, 122 kontrol berikut mengevaluasi sumber daya Azure Anda. Kontrol didistribusikan di dua standar:

- CIS Microsoft Azure Foundations Benchmark v4.0 - 96 kontrol dipetakan ke bagian CIS tertentu
- Azure Foundational Best Practices — 26 kontrol yang mencakup praktik terbaik keamanan tambahan

> **Note**
>
> Kontrol yang mengevaluasi ID Microsoft Entra dan sumber daya Microsoft Graph memerlukan cakupan wilayah global untuk disertakan dalam konfigurasi integrasi Anda.

Kontrol Azure yang tersedia

Judul kontrol	Tipe sumber daya	Standar
Aplikasi Azure Container dengan identitas terkelola diaktifkan harus mengikuti hak istimewa paling sedikit	`microsoft.app/containerapps`	Praktik Terbaik Dasar Azure
Aplikasi Kontainer Azure tidak boleh meneruskan kredensyal Azure SDK sebagai variabel lingkungan	`microsoft.app/containerapps`	Praktik Terbaik Dasar Azure
Aplikasi Kontainer Azure seharusnya tidak mengaktifkan ingress eksternal	`microsoft.app/containerapps`	Praktik Terbaik Dasar Azure
Lingkungan Aplikasi Azure Container seharusnya tidak memiliki akses NSG yang tidak terbatas	`microsoft.app/containerapps`	Praktik Terbaik Dasar Azure
Lingkungan terkelola Azure Container App seharusnya tidak mengaktifkan IP publik	`microsoft.app/managedenvironments`	Praktik Terbaik Dasar Azure

Judul kontrol	Tipe sumber daya	Standar
Penetapan peran Azure seharusnya tidak memberikan akses admin yang luas pada cakupan langganan	`microsoft.authorization/roleassignments`	Praktik Terbaik Dasar Azure
Penetapan peran Azure tidak boleh memberikan peran Administrator Akses Pengguna	`microsoft.authorization/roleassignments`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Definisi peran khusus Azure seharusnya tidak memiliki izin administratif wildcard	`microsoft.authorization/roledefinitions`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Penetapan kebijakan Microsoft Cloud Security Benchmark harus mengaktifkan mode penegakan	`microsoft.authorization/policyassignments`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Cluster Azure Kubernetes Service (AKS) seharusnya tidak memiliki server API yang dapat diakses publik tanpa batasan IP	`microsoft.containerservice/managedclusters`	Praktik Terbaik Dasar Azure
Cluster Azure Kubernetes Service (AKS) harus mengenkripsi rahasia Kubernetes saat istirahat	`microsoft.containerservice/managedclusters`	Praktik Terbaik Dasar Azure
Cluster Azure Kubernetes Service (AKS) harus menjalankan versi Kubernetes yang didukung	`microsoft.containerservice/managedclusters`	Praktik Terbaik Dasar Azure
Akun Azure Cosmos DB harus mengaktifkan pencadangan berkelanjutan	`microsoft.documentdb/databaseaccounts`	Praktik Terbaik Dasar Azure
Database Azure untuk server fleksibel MySQL harus menonaktifkan akses jaringan publik	`microsoft.dbformysql/flexibleservers`	Praktik Terbaik Dasar Azure

Judul kontrol	Tipe sumber daya	Standar
Ruang kerja Azure Databricks harus digunakan di jaringan virtual yang dikelola pelanggan	`microsoft.databricks/workspaces`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Ruang kerja Azure Databricks harus memiliki pengiriman log diagnostik yang dikonfigurasi	`microsoft.databricks/workspaces`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Ruang kerja Azure Databricks harus menggunakan kunci yang dikelola pelanggan untuk enkripsi disk terkelola	`microsoft.databricks/workspaces`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan otorisasi Microsoft Entra ID harus melarang pengguna default mendaftarkan aplikasi	`microsoft.graph/policies/authorizationpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
ID Azure Entra harus mengaktifkan default keamanan	`microsoft.graph/policies/identitysecuritydefaultsenforcementpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Penyewa Microsoft Entra harus memiliki kebijakan Akses Bersyarat yang memblokir akses dari lokasi geografis yang tidak diizinkan	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Penyewa Microsoft Entra harus memiliki kebijakan Akses Bersyarat yang memblokir alur otentikasi kode perangkat	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan akses bersyarat Azure harus mewajibkan MFA untuk semua pengguna	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Penyewa Microsoft Entra harus memerlukan otentikasi multifaktor untuk login berisiko melalui kebijakan Akses Bersyarat	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Penyewa Azure harus meminta MFA melalui Akses Bersyarat untuk API Manajemen Layanan Azure	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Setidaknya satu kebijakan Akses Bersyarat harus mewajibkan MFA untuk Microsoft Admin Portal	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan otorisasi Microsoft Entra harus membatasi pengguna non-admin untuk membuat penyewa	`microsoft.graph/policies/authorizationpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan metode otentikasi Microsoft Entra ID harus menetapkan periode konfirmasi ulang ke nilai bukan nol	`microsoft.graph/policies/authenticationmethodspolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan otorisasi Microsoft Entra harus membatasi persetujuan pengguna untuk aplikasi	`microsoft.graph/policies/authorizationpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan otorisasi Azure harus membatasi persetujuan pengguna untuk aplikasi penerbit terverifikasi	`microsoft.graph/policies/authorizationpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan otorisasi Microsoft Entra harus membatasi akses pengguna tamu ke objek direktori mereka sendiri	`microsoft.graph/policies/authorizationpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kebijakan otorisasi Azure harus membatasi undangan tamu hanya untuk peran admin	`microsoft.graph/policies/authorizationpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Kebijakan otorisasi Azure harus membatasi pembuatan grup keamanan untuk administrator	`microsoft.graph/policies/authorizationpolicy`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Penyewa Microsoft Entra harus memerlukan otentikasi multi-faktor untuk mendaftar atau bergabung dengan perangkat	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Peran direktori Microsoft Entra ID harus memiliki antara 2 dan 4 Administrator Global	`microsoft.graph/directoryrole`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Pengaturan grup ID Azure Entra harus membatasi pembuatan grup ke administrator	`microsoft.graph/organization`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki pengaturan diagnostik yang dikonfigurasi untuk log aktivitas	`microsoft.insights/diagnosticsettings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk membuat penetapan kebijakan	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk penghapusan penetapan kebijakan	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk membuat atau memperbarui operasi Grup Keamanan Jaringan	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Langganan Azure harus memiliki peringatan log aktivitas untuk penghapus an Grup Keamanan Jaringan	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk membuat atau memperbarui Solusi Keamanan	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk penghapus an Solusi Keamanan	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk membuat atau memperbarui aturan firewall server SQL	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk menghapus aturan firewall server SQL	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas yang dikonfigu rasi untuk operasi Buat atau Perbarui Alamat IP Publik	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk penghapus an alamat IP Publik	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki peringatan log aktivitas untuk insiden Service Health	`microsoft.insights/activitylogalerts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki setidaknya satu komponen Application Insights yang dikonfigurasi	`microsoft.insights/components`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Azure Key Vaults harus mengaktifkan soft delete dan purge protection	`microsoft.keyvault/vaults`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Azure Key Vaults harus mengaktifkan kontrol akses berbasis peran	`microsoft.keyvault/vaults`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Azure Key Vaults harus menonaktifkan akses jaringan publik saat menggunakan titik akhir pribadi	`microsoft.keyvault/vaults`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Azure Key Vaults harus menggunakan titik akhir pribadi	`microsoft.keyvault/vaults`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Azure Key Vaults harus mengaktifkan perlindungan pembersihan	`microsoft.keyvault/vaults`	Praktik Terbaik Dasar Azure
Azure Key Vaults harus membatasi akses jaringan	`microsoft.keyvault/vaults`	Praktik Terbaik Dasar Azure
Azure Key Vaults seharusnya mengaktif kan logging AuditEvent	`microsoft.keyvault/vaults`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kunci Azure Key Vault di brankas RBAC harus memiliki tanggal kedaluwarsa yang ditetapkan	`microsoft.keyvault/vaults/keys`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kunci Azure Key Vault di brankas non-RBAC harus memiliki tanggal kedaluwar sa yang ditetapkan	`microsoft.keyvault/vaults/keys`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Rahasia Azure Key Vault di brankas harus memiliki RBAC-enabled tanggal kedaluwarsa yang ditetapkan	`microsoft.keyvault/vaults/secrets`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Rahasia Azure Key Vault di brankas non-RBAC harus memiliki tanggal kedaluwarsa yang ditetapkan	`microsoft.keyvault/vaults/secrets`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Tombol Azure Key Vault harus mengaktifkan rotasi otomatis	`microsoft.keyvault/vaults/keys`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Grup keamanan jaringan Azure harus membatasi akses RDP masuk dari internet	`microsoft.network/networksecuritygroups`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Grup keamanan jaringan Azure harus membatasi akses UDP masuk dari internet	`microsoft.network/networksecuritygroups`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Grup keamanan jaringan Azure harus membatasi akses HTTP masuk dari internet	`microsoft.network/networksecuritygroups`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Subnet Azure Application Gateway seharusnya tidak memiliki akses NSG yang tidak terbatas	`microsoft.network/networksecuritygroups`	Praktik Terbaik Dasar Azure
Grup keamanan jaringan Azure harus memiliki aturan penolakan semua eksplisit	`microsoft.network/networksecuritygroups`	Praktik Terbaik Dasar Azure
Grup keamanan jaringan Azure tidak boleh mengizinkan akses masuk tanpa batas ke port terbatas	`microsoft.network/networksecuritygroups`	Praktik Terbaik Dasar Azure
Log aliran Azure Network Watcher harus mengaktifkan pencatatan aliran jaringan virtual dengan analitik lalu lintas yang dikirim ke Log Analytics	`microsoft.network/networkwatchers/flowlogs`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Grup keamanan jaringan Azure harus membatasi akses SSH dari internet	`microsoft.network/networksecuritygroups`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki setidaknya satu host Azure Bastion	`microsoft.network/bastionhosts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender untuk Server	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Mesin harus memiliki solusi penilaian kerentanan yang sehat yang digunakan di Microsoft Defender for Cloud	`microsoft.security/assessments`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki integrasi perlindungan titik akhir dengan Microsoft Defender for Cloud diaktifkan	`microsoft.security/settings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus memiliki pemindaian tanpa agen untuk mesin yang diaktifkan di Microsoft Defender untuk Server	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Pemantauan Integritas File di Defender for Server	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender for Containers	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender for Storage	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Langganan Azure harus mengaktifkan Microsoft Defender untuk Layanan Aplikasi	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender untuk Azure Cosmos DB	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender untuk basis data relasional sumber terbuka	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender untuk Database Azure SQL	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender untuk Server SQL di Mesin	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender untuk Key Vault	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender for Resource Manager	`microsoft.security/pricings`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Mesin virtual harus memiliki penilaian pembaruan sistem yang dilaporkan sehat oleh Microsoft Defender for Cloud	`microsoft.security/assessments`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kontak keamanan Microsoft Defender for Cloud harus memberi tahu peran peringatan Pemilik	`microsoft.security/securitycontacts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Microsoft Defender untuk kontak keamanan Cloud harus memiliki alamat email tambahan yang dikonfigurasi	`microsoft.security/securitycontacts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kontak keamanan Azure harus mengaktifkan notifikasi email peringatan dengan tingkat keparahan minimum yang cukup inklusif	`microsoft.security/securitycontacts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Kontak keamanan Azure harus mengaktifkan pemberitahuan email jalur serangan dengan tingkat risiko yang dikonfigurasi	`microsoft.security/securitycontacts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Langganan Azure harus mengaktifkan Microsoft Defender untuk IoT	`microsoft.security/iotsecuritysolutions`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Server Azure SQL harus menonaktifkan akses jaringan publik	`microsoft.sql/servers`	Praktik Terbaik Dasar Azure
Server SQL harus memiliki administrator Azure Active Directory yang dikonfigurasi	`microsoft.sql/servers`	Praktik Terbaik Dasar Azure
Database Azure SQL harus mengaktifkan cadangan geo-redundan	`microsoft.sql/servers/databases`	Praktik Terbaik Dasar Azure
Server Azure SQL tidak boleh menggunakan nama akun administrator default	`microsoft.sql/servers`	Praktik Terbaik Dasar Azure
Instans Terkelola Azure SQL harus mengaktifkan peningkatan versi minor otomatis	`microsoft.sql/managedinstances`	Praktik Terbaik Dasar Azure
Akun Azure Storage harus menggunakan kunci yang dikelola pelanggan untuk enkripsi	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Layanan file akun Azure Storage harus mengaktifkan soft delete untuk berbagi file	`microsoft.storage/storageaccounts/fileservices`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Pembagian file akun Azure Storage harus membatasi versi protokol SMB ke SMB 3.1.1	`microsoft.storage/storageaccounts/fileservices`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus menggunakan algoritma enkripsi saluran SMB yang aman untuk berbagi file	`microsoft.storage/storageaccounts/fileservices`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus memiliki pengingat rotasi kunci yang dikonfigurasi	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage seharusnya menonaktifkan akses kunci bersama	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus menggunakan titik akhir pribadi untuk akses	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus menonaktifkan akses jaringan publik	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus memiliki akses jaringan default yang disetel untuk ditolak	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun penyimpanan harus default ke otorisasi Microsoft Entra di portal Azure	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Akun Azure Storage harus memerlukan transfer aman	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus mengizinkan layanan Azure tepercaya untuk melewati aturan jaringan	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus dikonfigurasi dengan versi TLS minimum yang diperlukan	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus menonaktifkan replikasi lintas penyewa	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus menonaktifkan akses blob anonim	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus membatasi penghapusan gumpalan permanen	`microsoft.storage/storageaccounts/blobservices`	Praktik Terbaik Dasar Azure
Akun penyimpanan Azure yang berisi log aktivitas harus dienkripsi dengan kunci yang dikelola pelanggan	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Layanan gumpalan akun Azure Storage harus mengaktifkan blob soft delete	`microsoft.storage/storageaccounts/blobservices`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Layanan gumpalan akun Azure Storage harus mengaktifkan versi	`microsoft.storage/storageaccounts/blobservices`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Judul kontrol	Tipe sumber daya	Standar
Layanan gumpalan akun Azure Storage harus mengaktifkan blob dan container soft delete	`microsoft.storage/storageaccounts/blobservices`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus menerapkan kunci penghapusan Azure Resource Manager	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus memiliki kunci manajer ReadOnly sumber daya	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Akun Azure Storage harus menggunakan penyimpanan geo-redundan	`microsoft.storage/storageaccounts`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0
Aplikasi Azure Function harus membatasi akses administratif	`microsoft.web/sites/config`	Praktik Terbaik Dasar Azure
Azure Functions seharusnya tidak mengizinkan pemanggilan pemicu HTTP anonim	`microsoft.web/sites/functions`	Praktik Terbaik Dasar Azure
Aplikasi web dan aplikasi fungsi Azure App Service tidak boleh menggunakan versi runtime yang tidak didukung	`microsoft.web/sites`	Praktik Terbaik Dasar Azure
Aplikasi Azure Function pada paket Premium atau Dedicated harus diintegrasikan dengan jaringan virtual	`microsoft.web/sites`	Praktik Terbaik Dasar Azure
Aplikasi web Azure App Service harus mengaktifkan log HTTP dalam pengaturan diagnostik	`microsoft.web/sites`	Tolok Ukur Yayasan Microsoft Azure CIS v4.0

Menghapus konektor Microsoft Azure di Security Hub CSPM

Setelah Anda membuat konektor Microsoft Azure di AWS Security Hub CSPM, Anda dapat menghapusnya kapan saja. Jika Anda menghapus konektor, Security Hub CSPM berhenti melakukan pemeriksaan manajemen postur dan pemantauan kerentanan untuk lingkungan Azure Anda. Security Hub CSPM juga berhenti menghasilkan temuan baru tentang lingkungan Anda. Temuan Anda yang ada dipertahankan selama 90 hari. Inventaris sumber daya tetap seperti ketika konektor dihapus dan dihapus setelah 90 hari.

Saat Anda menghapus konektor, perhatikan hal berikut:

- Security Hub CSPM tidak menghapus registrasi aplikasi Azure dan infrastruktur Event Hub di lingkungan Azure Anda. Anda harus menghapusnya secara manual, langsung di Microsoft Azure. Untuk mempelajari caranya, lihat Menghapus aplikasi di dokumentasi Microsoft Azure.
- Jika konektor adalah konektor yang dikelola pelanggan dan konektor terkait layanan juga ada, menghapus konektor yang dikelola pelanggan tidak memengaruhi konektor yang ditautkan layanan. Security Hub CSPM terus menerima temuan manajemen postur melalui konektor terkait layanan.
- Temuan yang ada bertransisi ke keadaan yang diarsipkan dalam 3-5 hari dan dihapus setelah periode retensi 90 hari.

Untuk menghapus konektor Azure

1. Buka konsol CSPM Security Hub.
2. Di panel navigasi, pilih Integrasi.
3. Pilih konektor Anda.
4. Pilih Hapus.
5. Saat diminta, konfirmasikan bahwa Anda ingin menghapus konektor.

Setelah penghapusan, Anda dapat secara opsional membersihkan sumber daya Azure yang dibuat selama penyiapan:

- Hapus pendaftaran aplikasi di Microsoft Entra ID.
- Hapus namespace Event Hub dan grup sumber daya.
- Hapus setelan diagnostik yang mengekspor Log Aktivitas dan Log Audit Entra ID.

Membuat dan memperbarui temuan di Security Hub CSPM

Dalam AWS Security Hub CSPM, tem uan adalah catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Sebuah temuan dapat berasal dari salah satu sumber berikut:

- Pemeriksaan keamanan untuk kontrol di Security Hub CSPM.
- integrasi dengan yang lain Layanan AWS.
- Integrasi dengan produk pihak ketiga.
- Integrasi khusus.

Security Hub CSPM menormalkan temuan dari semua sumber ke dalam sintaks standar dan format yang disebut AWS Security Finding Format (ASFF). Untuk informasi terperinci tentang format ini, termasuk deskripsi masing-masing bidang ASFF, lihatAWS Format Penemuan Keamanan (ASFF). Jika Anda mengaktifkan agregasi lintas wilayah, Security Hub CSPM juga mengumpulkan temuan baru dan diperbarui secara otomatis dari semua Wilayah yang ditautkan ke Wilayah agregasi yang Anda tentukan. Untuk informasi selengkapnya, lihat Memahami agregasi lintas wilayah di Security Hub CSPM.

Setelah temuan dibuat, dapat diperbarui sebagai berikut:

- Penyedia pencarian dapat menggunakan BatchImportFindings operasi Security Hub CSPM API untuk memperbarui informasi umum tentang temuan tersebut. Mencari penyedia hanya dapat memperbarui temuan yang mereka buat.
- Pelanggan dapat menggunakan konsol CSPM Security Hub atau pen BatchUpdateFindings goperasian Security Hub CSPM API untuk memperbarui status penyelidikan terhadap temuan tersebut. `BatchUpdateFindings`Operasi ini juga dapat digunakan oleh SIEM, tiket, manajemen insiden, SOAR, atau jenis alat lain atas nama pelanggan.

Untuk mengurangi kebisingan pencarian dan merampingkan pelacakan dan analisis temuan individu, Security Hub CSPM secara otomatis menghapus temuan yang belum diperbarui baru-baru ini. Waktu di mana Security Hub CSPM melakukan ini tergantung pada apakah temuan aktif atau diarsipkan:

- Tem uan aktif adalah temuan yang status catatannya (`RecordState`)`ACTIVE`. Security Hub CSPM menyimpan temuan aktif selama 90 hari. Jika temuan aktif belum diperbarui selama 90 hari, temuan tersebut akan kedaluwarsa dan Security Hub CSPM menghapusnya secara permanen.

- Tem uan yang diarsipkan adalah temuan yang status cat `RecordState` atannya ()`ARCHIVED`. Security Hub CSPM menyimpan temuan yang diarsipkan selama 30 hari. Jika temuan yang diarsipkan belum diperbarui selama 30 hari, temuan tersebut akan kedaluwarsa dan Security Hub CSPM menghapusnya secara permanen.

Untuk temuan kontrol, yang merupakan temuan yang dihasilkan Security Hub CSPM dari pemeriksaan keamanan untuk kontrol, Security Hub CSPM menentukan apakah temuan telah kedaluwarsa berdasarkan nilai untuk `UpdatedAt` bidang temuan. Jika nilai ini lebih dari 90 hari yang lalu untuk temuan aktif, Security Hub CSPM menghapus temuan secara permanen. Jika nilai ini lebih dari 30 hari yang lalu untuk temuan yang diarsipkan, Security Hub CSPM menghapus temuan secara permanen.

Untuk semua jenis temuan lainnya, Security Hub CSPM menentukan apakah temuan telah kedaluwarsa berdasarkan nilai untuk `ProcessedAt` dan `UpdatedAt` bidang temuan. Security Hub CSPM membandingkan nilai untuk bidang ini dan menentukan mana yang lebih baru. Jika nilai yang lebih baru lebih dari 90 hari yang lalu untuk temuan aktif, Security Hub CSPM menghapus temuan secara permanen. Jika nilai yang lebih baru lebih dari 30 hari yang lalu untuk temuan yang diarsipkan, Security Hub CSPM menghapus temuan secara permanen. Penyedia pencarian dapat mengubah nilai untuk `UpdatedAt` bidang satu atau lebih temuan dengan menggunakan BatchImportFindings operasi Security Hub CSPM API.

Untuk penyimpanan temuan jangka panjang, Anda dapat mengekspor temuan ke bucket S3. Anda dapat melakukan ini dengan menggunakan tindakan khusus dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat Menggunakan EventBridge untuk respon otomatis dan remediasi.

Topik

- BatchImportFindings untuk menemukan penyedia
- BatchUpdateFindings untuk pelanggan
- Meninjau detail dan riwayat temuan di Security Hub CSPM
- Penyaringan temuan di Security Hub CSPM
- Pengelompokan temuan di Security Hub CSPM
- Mengatur status alur kerja temuan di Security Hub CSPM
- Mengirim temuan ke tindakan CSPM Hub Keamanan kustom
- AWS Format Penemuan Keamanan (ASFF)

BatchImportFindings untuk menemukan penyedia

Penyedia pencarian dapat menggunakan BatchImportFindings operasi untuk membuat temuan baru di AWS Security Hub CSPM. Mereka juga dapat menggunakan operasi ini untuk memperbarui temuan yang mereka buat. Penyedia pencarian tidak dapat memperbarui temuan yang tidak mereka buat.

Pelanggan, SIEM, tiket, SOAR, dan jenis alat lainnya harus menggunakan BatchUpdateFindings operasi untuk membuat pembaruan terkait dengan penyelidikan mereka terhadap temuan dari penyedia pencarian. Untuk informasi selengkapnya, lihat the section called “BatchUpdateFindings untuk pelanggan”.

Ketika Security Hub CSPM menerima `BatchImportFindings` permintaan untuk membuat atau memperbarui temuan, itu secara otomatis menghasilkan Security Hub Findings - Imported peristiwa di Amazon. EventBridge Anda dapat mengambil tindakan otomatis pada acara itu. Untuk informasi selengkapnya, lihat the section called “Respon dan remediasi otomatis”.

Prasyarat untuk menggunakan **`BatchImportFindings`**

`BatchImportFindings`harus dipanggil oleh salah satu dari berikut ini:

- Akun yang terkait dengan temuan. Pengidentifikasi akun terkait harus sesuai dengan nilai `AwsAccountId` atribut untuk temuan.
- Akun yang diizinkan terdaftar sebagai integrasi mitra CSPM Security Hub resmi.

Security Hub CSPM hanya dapat menerima pencarian pembaruan untuk akun yang mengaktifkan Security Hub CSPM. Penyedia pencarian juga harus diaktifkan. Jika Security Hub CSPM dinonaktifkan, atau integrasi penyedia pencarian tidak diaktifkan, maka temuan dikembalikan dalam `FailedFindings` daftar, dengan kesalahan`InvalidAccess`.

Menentukan apakah akan membuat atau memperbarui temuan

Untuk menentukan apakah akan membuat atau memperbarui temuan, Security Hub CSPM memeriksa bidang tersebut`ID`. Jika nilai `ID` tidak cocok dengan temuan yang ada, Security Hub CSPM membuat temuan baru.

Jika `ID` cocok dengan temuan yang ada, Security Hub CSPM memeriksa `UpdatedAt` bidang untuk pembaruan, dan melanjutkan sebagai berikut:

- Jika `UpdatedAt` pada pembaruan cocok atau terjadi sebelumnya `UpdatedAt` pada temuan yang ada, Security Hub CSPM mengabaikan permintaan pembaruan.
- Jika `UpdatedAt` pembaruan terjadi setelah temuan `UpdatedAt` yang ada, Security Hub CSPM memperbarui temuan yang ada.

Pembatasan untuk menemukan pembaruan dengan **`BatchImportFindings`**

Penyedia pencarian tidak dapat digunakan `BatchImportFindings` untuk memperbarui atribut berikut dari temuan yang ada:

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM mengabaikan konten apa pun yang disediakan dalam `BatchImportFindings` permintaan untuk atribut ini. Pelanggan, atau entitas yang bertindak atas nama mereka (seperti alat tiket), dapat menggunakannya `BatchUpdateFindings` untuk memperbarui atribut ini.

Memperbarui temuan dengan FindingProviderFields

Penyedia pencarian juga tidak boleh digunakan `BatchImportFindings` untuk memperbarui atribut tingkat atas berikut dalam Format Penem AWS uan Keamanan (ASFF):

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Sebaliknya, penyedia pencarian harus menggunakan `FindingProviderFields` objek untuk memberikan nilai untuk atribut ini.

Contoh

```
"FindingProviderFields": {
```

```
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

Untuk `BatchImportFindings` permintaan, Security Hub CSPM menangani nilai di atribut tingkat atas dan sebagai berikut. `FindingProviderFields`

(Preferred) **`BatchImportFindings`** memberikan nilai untuk atribut di **`FindingProviderFields`**, tetapi tidak memberikan nilai untuk atribut tingkat atas yang sesuai.

Misalnya, `BatchImportFindings` menyediakan`FindingProviderFields.Confidence`, tetapi tidak menyediakan`Confidence`. Ini adalah opsi yang disukai untuk `BatchImportFindings` permintaan.

Security Hub CSPM memperbarui nilai atribut di. `FindingProviderFields`

Ini mereplikasi nilai ke atribut tingkat atas hanya jika atribut belum diperbarui oleh. `BatchUpdateFindings`

`BatchImportFindings`memberikan nilai untuk atribut tingkat atas, tetapi tidak memberikan nilai untuk atribut yang sesuai di**`FindingProviderFields`**.

Misalnya, `BatchImportFindings` menyediakan`Confidence`, tetapi tidak menyediakan`FindingProviderFields.Confidence`.

Security Hub CSPM menggunakan nilai untuk memperbarui atribut di. `FindingProviderFields` Ini mengganti nilai yang ada.

Security Hub CSPM memperbarui atribut tingkat atas hanya jika atribut belum diperbarui oleh. `BatchUpdateFindings`

`BatchImportFindings`memberikan nilai untuk atribut tingkat atas dan atribut yang sesuai di**`FindingProviderFields`**.

Misalnya, `BatchImportFindings` menyediakan keduanya `Confidence` dan`FindingProviderFields.Confidence`.

Untuk temuan baru, Security Hub CSPM menggunakan nilai in `FindingProviderFields` untuk mengisi atribut tingkat atas dan atribut yang sesuai di. `FindingProviderFields` Itu tidak menggunakan nilai atribut tingkat atas yang disediakan.

Untuk temuan yang ada, Security Hub CSPM menggunakan kedua nilai tersebut. Namun, ini memperbarui nilai atribut tingkat atas hanya jika atribut belum diperbarui oleh`BatchUpdateFindings`.

BatchUpdateFindings untuk pelanggan

AWS Pelanggan Security Hub CSPM, dan entitas yang bertindak atas nama mereka, dapat menggunakan BatchUpdateFindings operasi untuk memperbarui informasi yang terkait dengan pemrosesan temuan Security Hub CSPM dari penyedia pencarian. Sebagai pelanggan, Anda dapat menggunakan operasi ini secara langsung. SIEM, ticketing, manajemen insiden, dan alat SOAR juga dapat menggunakan operasi ini atas nama pelanggan.

Anda tidak dapat menggunakan `BatchUpdateFindings` operasi untuk membuat temuan baru. Namun, Anda dapat menggunakannya untuk memperbarui hingga 100 temuan yang ada sekaligus. Dalam `BatchUpdateFindings` permintaan, Anda menentukan temuan mana yang akan diperbarui, bidang Format AWS Penemuan Keamanan (ASFF) mana yang akan diperbarui untuk temuan, dan nilai baru untuk bidang tersebut. Security Hub CSPM kemudian memperbarui temuan seperti yang ditentukan dalam permintaan Anda. Proses ini dapat memakan waktu beberapa menit. Jika Anda memperbarui temuan dengan menggunakan `BatchUpdateFindings` operasi, pembaruan Anda tidak memengaruhi nilai yang ada untuk `UpdatedAt` bidang temuan.

Ketika Security Hub CSPM menerima `BatchUpdateFindings` permintaan untuk memperbarui temuan, itu secara otomatis menghasilkan Security Hub Findings – Imported peristiwa di Amazon. EventBridge Anda dapat menggunakan acara ini secara opsional untuk mengambil tindakan otomatis pada temuan yang ditentukan. Untuk informasi selengkapnya, lihat the section called “Respon dan remediasi otomatis”.

Bidang yang tersedia untuk BatchUpdateFindings

Jika Anda masuk ke akun administrator CSPM Security Hub, Anda dapat menggunakannya `BatchUpdateFindings` untuk memperbarui temuan yang dihasilkan oleh akun administrator atau akun anggota. Akun anggota dapat digunakan `BatchUpdateFindings` untuk memperbarui temuan hanya untuk akun mereka.

Pelanggan dapat menggunakan `BatchUpdateFindings` untuk memperbarui bidang dan objek berikut:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Mengkonfigurasi akses ke BatchUpdateFindings

Anda dapat mengonfigurasi kebijakan AWS Identity and Access Management (IAM) untuk membatasi akses penggunaan `BatchUpdateFindings` untuk memperbarui bidang pencarian dan nilai bidang.

Dalam pernyataan untuk membatasi akses ke`BatchUpdateFindings`, gunakan nilai-nilai berikut:

- `Action`adalah `securityhub:BatchUpdateFindings`
- `Effect`adalah `Deny`
- Untuk`Condition`, Anda dapat menolak `BatchUpdateFindings` permintaan berdasarkan hal berikut:
  - Temuan ini mencakup bidang tertentu.
  - Temuan ini mencakup nilai bidang tertentu.

Kunci syarat

Ini adalah kunci kondisi untuk membatasi akses ke`BatchUpdateFindings`.

Bidang ASFF

Kunci kondisi untuk bidang ASFF adalah sebagai berikut:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Ganti *<fieldName>* dengan bidang ASFF. Saat mengonfigurasi akses ke`BatchUpdateFindings`, sertakan satu atau lebih bidang ASFF tertentu dalam kebijakan IAM Anda, bukan bidang tingkat induk. Misalnya, untuk membatasi akses ke `Workflow.Status` bidang, Anda harus menyertakan `securityhub:ASFFSyntaxPath/Workflow.Status` dalam kebijakan, bukan bidang `Workflow` tingkat induk.

Melarang semua pembaruan ke bidang

Untuk mencegah pengguna melakukan pembaruan apa pun ke bidang tertentu, gunakan kondisi seperti ini:

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
                }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak `BatchUpdateFindings` dapat digunakan untuk memperbarui `Workflow.Status` bidang temuan.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
    }
```

```
}
```

Melarang nilai bidang tertentu

Untuk mencegah pengguna menyetel bidang ke nilai tertentu, gunakan kondisi seperti ini:

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak `BatchUpdateFindings` dapat digunakan untuk mengatur `Workflow.Status` ke`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

Anda juga dapat memberikan daftar nilai yang tidak diizinkan.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

Misalnya, pernyataan berikut menunjukkan bahwa tidak `BatchUpdateFindings` dapat digunakan untuk mengatur `Workflow.Status` ke salah satu `RESOLVED` atau`SUPPRESSED`.

```
{
    "Sid": "VisualEditor0",
```

```
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

Meninjau detail dan riwayat temuan di Security Hub CSPM

Dalam AWS Security Hub CSPM, tem uan adalah catatan yang dapat diamati dari pemeriksaan keamanan atau deteksi terkait keamanan. Security Hub CSPM menghasilkan temuan ketika menyelesaikan pemeriksaan keamanan kontrol dan ketika menelan temuan dari produk terintegrasi Layanan AWS atau pihak ketiga. Setiap temuan mencakup riwayat perubahan dan detail lainnya, seperti peringkat keparahan dan informasi tentang sumber daya yang terpengaruh.

Anda dapat meninjau riwayat dan detail lain dari temuan individu di konsol CSPM Hub Keamanan atau secara terprogram dengan Security Hub CSPM API atau. AWS CLI

Untuk membantu Anda merampingkan analisis, konsol CSPM Security Hub menampilkan panel pencarian saat Anda memilih temuan tertentu. Panel mencakup menu dan tab yang berbeda untuk meninjau detail spesifik dari suatu temuan.

Menu Tindakan

Dari menu ini, Anda dapat meninjau JSON lengkap dari temuan atau menambahkan catatan. Sebuah temuan hanya dapat memiliki satu catatan yang dilampirkan padanya pada satu waktu. Menu ini juga menyediakan opsi untuk mengatur status alur kerja temuan atau mengirim temuan ke tindakan khusus di Amazon EventBridge.

Selidiki menu

Dari menu ini, Anda dapat menyelidiki temuan di Amazon Detective. Detektif mengekstrak entitas, seperti alamat IP dan AWS pengguna, dari temuan dan memvisualisasikan aktivitas mereka. Anda dapat menggunakan aktivitas entitas sebagai titik awal untuk menyelidiki penyebab dan dampak temuan.

Tab Ikhtisar

Tab ini memberikan ringkasan temuan. Misalnya, Anda dapat menentukan kapan temuan dibuat dan terakhir diperbarui, di akun mana itu ada, dan sumber temuan. Untuk temuan kontrol, tab ini juga menampilkan nama AWS Config aturan terkait dan tautan ke panduan remediasi dalam dokumentasi CSPM Security Hub.

Dalam snapshot Sumber daya pada tab I khtisar, Anda bisa mendapatkan gambaran singkat tentang sumber daya yang terlibat dalam temuan. Untuk beberapa sumber daya, ini termasuk opsi sumber daya terbuka, yang menautkan langsung ke sumber daya yang terkena dampak di Layanan AWS konsol yang relevan. Cup li kan Riwayat menunjukkan hingga dua perubahan yang dilakukan pada temuan pada tanggal terbaru di mana riwayat sedang dilacak. Misalnya, jika Anda membuat satu perubahan kemarin dan satu lagi hari ini, snapshot menunjukkan perubahan hari ini. Untuk meninjau entri sebelumnya, beralih ke tab Riwayat.

Baris Kepatu han diperluas untuk menampilkan detail selengkapnya. Misalnya, jika kontrol menyertakan parameter, Anda dapat meninjau nilai parameter yang saat ini digunakan CSPM Security Hub saat melakukan pemeriksaan keamanan untuk kontrol tersebut.

Tab sumber daya

Tab ini memberikan rincian tentang sumber daya yang terlibat dalam temuan. Jika Anda masuk ke akun yang memiliki sumber daya, Anda dapat meninjau sumber daya di Layanan AWS konsol yang berlaku. Jika Anda bukan pemilik sumber daya, tab ini menampilkan Akun AWS ID untuk pemilik.

Bar is Detail menampilkan detail spesifik sumber daya dalam temuan. Ini menunjukkan ResourceDetails bagian temuan dalam format JSON.

Bar is Tag menunjukkan kunci tag dan nilai yang ditetapkan ke sumber daya yang terlibat dalam penemuan. Sumber daya yang didukung oleh pen GetResources goperasian API Pen AWS Resource Groups andaan dapat diberi tag. Security Hub CSPM memanggil operasi ini dengan menggunakan peran terkait layanan saat memproses temuan baru atau yang diperbarui, dan mengambil tag sumber daya jika `Resource.Id` bidang Format Penemuan AWS Keamanan (ASFF) diisi dengan ARN sumber daya. Security Hub CSPM mengabaikan ID sumber daya yang tidak valid. Untuk informasi selengkapnya tentang penyertaan tag sumber daya dalam temuan, lihatTanda.

Tab Riwayat

Tab ini melacak sejarah temuan. Menemukan riwayat tersedia untuk temuan aktif dan diarsipkan. Ini memberikan jejak perubahan yang tidak dapat diubah yang dibuat pada temuan dari waktu ke waktu, termasuk bidang ASFF apa yang diubah, kapan perubahan terjadi, dan oleh pengguna mana. Setiap halaman pada tab menampilkan hingga 20 perubahan. Perubahan yang lebih baru ditampilkan terlebih dahulu.

Untuk temuan aktif, menemukan riwayat tersedia hingga 90 hari. Untuk temuan yang diarsipkan, riwayat pencarian tersedia hingga 30 hari. Menemukan riwayat mencakup perubahan yang dibuat secara manual, atau otomatis oleh aturan otomatisasi CSPM Security Hub. Itu tidak termasuk perubahan pada bidang stempel waktu tingkat atas, seperti bidang dan. `CreatedAt` `UpdatedAt`

Jika Anda masuk ke akun administrator CSPM Security Hub, pencarian riwayat adalah untuk akun administrator dan semua akun anggota.

Tab Ancaman

Tab ini mencakup data dari Action, Malware, dan ProcessDetails objek ASFF, termasuk jenis ancaman dan apakah sumber daya adalah target atau aktor. Rincian ini biasanya berlaku untuk temuan yang berasal dari Amazon GuardDuty.

Tab kerentanan

Tab ini menampilkan data dari Vulnerability objek ASFF, termasuk apakah ada eksploitasi atau perbaikan yang tersedia terkait dengan temuan. Rincian ini biasanya berlaku untuk temuan yang berasal dari Amazon Inspector.

Baris pada setiap tab menyertakan opsi salinan atau filter. Misalnya, jika Anda membuka panel untuk temuan yang memiliki status alur kerja Diberit ah ukan, Anda dapat memilih opsi filter di sebelah baris status alur kerja. Jika Anda memilih Tampilkan semua temuan dengan nilai ini, Security Hub CSPM memfilter tabel temuan dan hanya menampilkan temuan dengan status alur kerja yang sama.

Meninjau detail dan sejarah temuan

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk meninjau detail pencarian di Security Hub CSPM.

Jika Anda mengaktifkan agregasi lintas wilayah dan masuk ke Wilayah agregasi, menemukan data mencakup data dari Wilayah agregasi dan Wilayah tertaut. Di Wilayah lain, menemukan data khusus

untuk Wilayah itu saja. Untuk informasi selengkapnya tentang agregasi lintas wilayah, lihatthe section called “Menggabungkan data di seluruh Wilayah”.

Security Hub CSPM console

Meninjau detail dan sejarah temuan

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Untuk menampilkan daftar pencarian, lakukan salah satu hal berikut:
   - Di panel navigasi, pilih Temuan. Tambahkan filter pencarian seperlunya untuk mempersempit daftar temuan.
   - Pada panel navigasi, silakan pilih Wawasan. Pilih wawasan. Kemudian, dalam daftar hasil, pilih hasil wawasan.
   - Di panel navigasi, pilih Integrasi. Pilih Lihat temuan untuk integrasi.
   - Di panel navigasi, pilih Kontrol.
3. Pilih temuan. Panel temuan menampilkan detail temuan.
4. Di panel pencarian, lakukan salah satu hal berikut:
   - Untuk meninjau detail spesifik untuk temuan tersebut, pilih tab.
   - Untuk mengambil tindakan pada temuan, pilih opsi dari menu T indakan.
   - Untuk menyelidiki temuan di Amazon Detective, pilih opsi In vestigate.

> **Note**
>
> Jika Anda berintegrasi dengan AWS Organizations dan Anda masuk ke akun anggota, panel pencarian menyertakan nama akun. Untuk akun anggota yang diundang secara manual, bukan melalui Organisasi, panel pencarian hanya menyertakan ID akun.

Security Hub CSPM API

Gunakan GetFindings operasi Security Hub CSPM API, atau jika Anda menggunakan AWS CLI, jalankan perintah get-findings. Anda dapat memberikan satu atau lebih nilai untuk `Filters` parameter untuk mempersempit temuan yang akan diambil.

Jika volume hasil terlalu besar, Anda dapat menggunakan `MaxResults` parameter untuk membatasi temuan ke angka tertentu dan `NextToken` parameter untuk mempaginasi temuan. Gunakan `SortCriteria` parameter untuk mengurutkan temuan berdasarkan bidang tertentu.

Misalnya, AWS CLI perintah berikut mengambil temuan yang cocok dengan kriteria filter yang ditentukan, dan mengurutkan hasil dalam urutan menurun berdasarkan `LastObservedAt` bidang. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-findings \
--filters '{"GeneratorId":[{"Value": "aws-
foundational","Comparison":"PREFIX"}],"WorkflowStatus": [{"Value":
 "NEW","Comparison":"EQUALS"}],"Confidence": [{"Gte": 85}]}' --sort-criteria
 '{"Field": "LastObservedAt","SortOrder": "desc"}' --page-size 5 --max-items 100
```

Untuk meninjau riwayat penemuan, gunakan GetFindingHistory operasi. Jika Anda menggunakan AWS CLI, jalankan get-finding-history perintah. Identifikasi temuan yang ingin Anda dapatkan riwayat dengan `Id` bidang `ProductArn` dan. Untuk informasi tentang bidang ini, lihat AwsSecurityFindingIdentifier. Setiap permintaan dapat mengambil riwayat hanya untuk satu temuan.

Misalnya, AWS CLI perintah berikut mengambil riwayat untuk temuan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-finding-history \
--region us-west-2 \
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-
west-2:123456789012:product/123456789012/default" \
--max-results 2 \
--start-time "2021-09-30T15:53:35.573Z" \
--end-time "2021-09-31T15:53:35.573Z"
```

PowerShell

Gunakan `Get-SHUBFinding` cmdlet. Secara opsional mengisi `Filter` parameter untuk mempersempit temuan yang akan diambil.

Misalnya, cmdlet berikut mengambil temuan yang cocok dengan filter yang ditentukan.

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> Jika Anda memfilter temuan berdasarkan `CompanyName` atau`ProductName`, Security Hub CSPM menggunakan nilai yang merupakan bagian dari objek `ProductFields` ASFF. Security Hub CSPM tidak menggunakan tingkat atas dan bidang`CompanyName`. `ProductName`

Penyaringan temuan di Security Hub CSPM

AWS Security Hub CSPM menghasilkan temuannya sendiri dari pemeriksaan keamanan dan menerima temuan dari produk terintegrasi. Anda dapat menampilkan daftar temuan di halaman Tem uan, Integrasi, dan Wawasan dari konsol CSPM Security Hub. Anda dapat menambahkan filter untuk mempersempit daftar pencarian sehingga daftar tersebut relevan dengan organisasi atau kasus penggunaan Anda.

Untuk informasi tentang penyaringan temuan untuk kontrol keamanan tertentu, lihatthe section called “Penyaringan dan penyortiran temuan kontrol”. Informasi di halaman ini berlaku untuk halaman Temuan, Wawasan, dan Integrasi.

Filter default untuk menemukan daftar

Secara default, daftar pencarian di konsol CSPM Hub Keamanan difilter berdasarkan `Workflow.Status` bidang `RecordState` dan dari AWS Security Finding Format (ASFF). Ini adalah tambahan untuk filter untuk wawasan atau integrasi tertentu.

Status rekaman menunjukkan apakah temuan aktif atau diarsipkan. Secara default, daftar temuan hanya menampilkan temuan aktif. Penyedia pencarian dapat mengarsipkan temuan jika tidak lagi aktif atau penting. Security Hub CSPM juga secara otomatis mengarsipkan temuan kontrol jika sumber daya terkait dihapus.

Status alur kerja menunjukkan status penyelidikan terhadap temuan. Secara default, daftar pencarian hanya menampilkan temuan dengan status alur kerja `NEW` atau`NOTIFIED`. Anda dapat memperbarui status alur kerja dari suatu temuan.

Petunjuk untuk menambahkan filter

Anda dapat memfilter daftar pencarian hingga sepuluh atribut. Untuk setiap atribut, Anda dapat memberikan hingga 20 nilai filter.

Saat memfilter daftar temuan, Security Hub CSPM menerapkan `AND` logika ke kumpulan filter. Penemuan hanya cocok jika cocok dengan semua filter yang disediakan. Misalnya, jika Anda menambahkan GuardDuty sebagai filter untuk nama Produk, dan `AwsS3Bucket` sebagai filter untuk jenis Sumber daya, Security Hub CSPM menampilkan temuan yang cocok dengan kedua kriteria ini.

Security Hub CSPM menerapkan `OR` logika ke filter yang menggunakan atribut yang sama tetapi nilai yang berbeda. Misalnya, jika Anda menambahkan keduanya GuardDuty dan Amazon Inspector sebagai nilai filter untuk nama Produk, Security Hub CSPM menampilkan temuan yang dihasilkan oleh salah satu GuardDuty atau Amazon Inspector.

Untuk menambahkan filter ke daftar temuan (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Untuk menampilkan daftar temuan, lakukan salah satu tindakan berikut dari panel navigasi:
   - Pilih Temuan.
   - Pilih Wawasan. Pilih wawasan. Kemudian, pada daftar hasil, pilih hasil wawasan.
   - Pilih Integrasi. Pilih Lihat temuan untuk integrasi.
3. Di kotak Tambah filter, pilih satu atau beberapa file untuk difilter.

   Saat Anda memfilter berdasarkan nama Perusahaan atau Nama Produk, konsol menggunakan tingkat atas `CompanyName` dan `ProductName` bidang Format Penemuan AWS Keamanan (ASFF). API menggunakan nilai-nilai yang bersarang di bawah`ProductFields`.
4. Pilih jenis pencocokan filter.

   Untuk filter string, Anda dapat memilih dari opsi berikut:

   - is — Temukan nilai yang persis cocok dengan nilai filter.
   - dimulai dengan — Temukan nilai yang dimulai dengan nilai filter.

- is not — Temukan nilai yang tidak cocok dengan nilai filter.
- tidak dimulai dengan — Temukan nilai yang tidak dimulai dengan nilai filter.

Untuk bidang Tag sumber daya, Anda dapat memfilter berdasarkan kunci atau nilai tertentu.

Untuk filter numerik, Anda dapat memilih apakah akan memberikan angka tunggal (Seder hana) atau rentang angka (Rentang).

Untuk filter tanggal atau waktu, Anda dapat memilih apakah akan memberikan jangka waktu dari tanggal dan waktu saat ini (Jendela ber gulir) atau rentang tanggal tertentu (Rentang tetap).

Menambahkan beberapa filter memiliki interaksi berikut:

- is dan dimulai dengan filter bergabung dengan OR. Nilai cocok jika berisi salah satu nilai filter. Misalnya, jika Anda menentukan label tingkat keparahan KRITIS dan label tingkat keparahan adalah TINGGI, hasilnya mencakup temuan kritis dan tingkat keparahan tinggi.
- tidak dan tidak dimulai dengan filter yang digabungkan oleh AND. Nilai hanya cocok jika tidak mengandung nilai-nilai filter tersebut. Misalnya, jika Anda menentukan label tingkat keparahan bukan RENDAH dan label tingkat keparahan bukan SEDANG, hasilnya tidak menyertakan temuan tingkat keparahan rendah atau sedang.

Jika Anda memiliki filter is pada bidang, Anda tidak dapat memiliki is not atau a tidak dimulai dengan filter pada bidang yang sama.

5. Tentukan nilai filter. Untuk filter string, nilai filter peka huruf besar/kecil.
6. Pilih Terapkan.

Untuk filter yang ada, Anda dapat mengubah jenis atau nilai kecocokan filter. Pada daftar pencarian yang difilter, pilih filter. Di kotak Edit filter, pilih jenis atau nilai kecocokan baru, lalu pilih Ter apkan.

Untuk menghapus filter, pilih ikon x. Daftar diperbarui secara otomatis untuk mencerminkan perubahan.

Pengelompokan temuan di Security Hub CSPM

Anda dapat mengelompokkan temuan di AWS Security Hub CSPM berdasarkan nilai atribut yang dipilih.

Saat Anda mengelompokkan temuan, daftar temuan diganti dengan daftar nilai untuk atribut yang dipilih dalam temuan yang cocok. Untuk setiap nilai, daftar menampilkan jumlah temuan yang cocok.

Misalnya, jika Anda mengelompokkan temuan berdasarkan Akun AWS ID, Anda akan melihat daftar pengidentifikasi akun, dengan jumlah temuan yang cocok untuk setiap akun.

Security Hub CSPM dapat menampilkan hingga 100 nilai untuk atribut yang dipilih. Jika ada lebih dari 100 nilai, Anda hanya melihat 100 yang pertama.

Saat Anda memilih nilai atribut, Security Hub CSPM menampilkan daftar temuan yang cocok untuk nilai tersebut.

Untuk mengelompokkan temuan dalam daftar temuan (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Untuk menampilkan daftar temuan, lakukan salah satu tindakan berikut dari panel navigasi:
   - Pilih Temuan.
   - Pilih Wawasan. Pilih wawasan. Kemudian, pada daftar hasil, pilih hasil wawasan.
   - Pilih Integrasi. Pilih Lihat temuan untuk integrasi.
3. Di drop-down Grup berdasarkan, pilih atribut yang akan digunakan untuk pengelompokan.

   Untuk menghapus atribut pengelompokan, pilih ikon x. Saat Anda menghapus atribut pengelompokan, daftar berubah dari daftar nilai atribut menjadi daftar temuan.

Mengatur status alur kerja temuan di Security Hub CSPM

Status alur kerja melacak kemajuan penyelidikan Anda ke dalam temuan. Status alur kerja khusus untuk temuan individu dan tidak memengaruhi pembuatan temuan baru. Misalnya, jika Anda mengubah status alur kerja temuan menjadi `SUPPRESSED` atau`RESOLVED`, perubahan Anda tidak mencegah CSPM Hub Keamanan menghasilkan temuan baru untuk masalah yang sama.

Status alur kerja temuan dapat menjadi salah satu nilai berikut.

BARU

Keadaan awal temuan sebelum Anda meninjaunya.

Temuan yang dicerna dari terintegrasi Layanan AWS AWS Config, seperti, memiliki `NEW` status awal.

Security Hub CSPM juga mengatur ulang status alur kerja dari salah satu `NOTIFIED` atau `RESOLVED` ke `NEW` dalam kasus berikut:

- `RecordState`perubahan dari `ARCHIVED` ke`ACTIVE`.
- `Compliance.Status`perubahan dari `PASSED` ke`FAILED`,`WARNING`, atau`NOT_AVAILABLE`.

Perubahan ini menyiratkan bahwa penyelidikan tambahan diperlukan.

DIBERITAHUKAN

Menunjukkan bahwa Anda memberi tahu pemilik sumber daya tentang masalah keamanan. Anda dapat menggunakan status ini ketika Anda bukan pemilik sumber daya, dan Anda memerlukan intervensi dari pemilik sumber daya untuk menyelesaikan masalah keamanan.

Jika salah satu hal berikut terjadi, status alur kerja diubah secara otomatis dari `NOTIFIED` menjadi`NEW`:

- `RecordState`perubahan dari `ARCHIVED` ke`ACTIVE`.
- `Compliance.Status`perubahan dari `PASSED` ke`FAILED`,`WARNING`, atau`NOT_AVAILABLE`.

DITEKAN

Menunjukkan bahwa Anda meninjau temuan dan tidak percaya bahwa tindakan apa pun diperlukan.

Status alur kerja tem `SUPPRESSED` uan tidak berubah jika `RecordState` berubah dari `ARCHIVED` ke`ACTIVE`.

TERSELESAIKAN

Temuan itu ditinjau dan diperbaiki dan sekarang dianggap diselesaikan.

Temuan tetap ada `RESOLVED` kecuali salah satu dari hal-hal berikut terjadi:

- `RecordState`perubahan dari `ARCHIVED` ke`ACTIVE`.
- `Compliance.Status`perubahan dari `PASSED` ke`FAILED`,`WARNING`, atau`NOT_AVAILABLE`.

Dalam kasus tersebut, status alur kerja secara otomatis diatur ulang ke`NEW`.

Untuk temuan dari kontrol, jika `Compliance.Status` ada`PASSED`, Security Hub CSPM secara otomatis menetapkan status alur kerja ke. `RESOLVED`

Mengatur status alur kerja temuan

Untuk mengubah status alur kerja dari satu atau beberapa temuan, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Jika Anda mengubah status alur kerja suatu temuan, perhatikan bahwa perlu beberapa menit bagi Security Hub CSPM untuk memproses permintaan Anda dan memperbarui temuan.

> **Tip**
>
> Anda juga dapat mengubah status alur kerja temuan secara otomatis dengan menggunakan aturan otomatisasi. Dengan aturan otomatisasi, Anda mengonfigurasi Security Hub CSPM untuk secara otomatis memperbarui status alur kerja temuan berdasarkan kriteria yang Anda tentukan. Untuk informasi selengkapnya, lihat Memahami aturan otomatisasi di Security Hub CSPM.

Untuk mengubah status alur kerja dari satu atau lebih temuan, pilih metode pilihan Anda dan ikuti langkah-langkahnya.

Security Hub CSPM console

Untuk mengubah status alur kerja temuan

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, lakukan salah satu hal berikut untuk menampilkan tabel temuan:
   - Pilih Temuan.
   - Pilih Wawasan. Kemudian pilih wawasan. Dalam hasil wawasan, pilih hasilnya.
   - Pilih Integrasi. Kemudian, di bagian untuk integrasi, pilih Lihat temuan.
   - Pilih standar keamanan. Kemudian, di bagian untuk standar, pilih Lihat hasil. Dalam tabel kontrol, pilih kontrol untuk menampilkan temuan untuk kontrol.
3. Di tabel temuan, pilih kotak centang untuk setiap temuan yang status alur kerjanya ingin diubah.
4. Di bagian atas halaman, pilih Status alur kerja, lalu pilih status alur kerja baru untuk temuan yang dipilih.
5. Dalam kotak dialog Setel status alur kerja, secara opsional masukkan catatan yang merinci alasan untuk mengubah status alur kerja. Kemudian pilih Setel status.

Security Hub CSPM API

Gunakan BatchUpdateFindings operasi. Berikan ID temuan dan ARN produk yang menghasilkan temuan. Anda bisa mendapatkan detail ini dengan menggunakan GetFindings operasi.

AWS CLI

Jalankan perintah batch-update-. Berikan ID temuan dan ARN produk yang menghasilkan temuan. Anda bisa mendapatkan detail ini dengan menjalankan perintah get-.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Contoh

```
aws securityhub batch-update-findings --finding-identifiers
 Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Mengirim temuan ke tindakan CSPM Hub Keamanan kustom

Anda dapat membuat tindakan kustom AWS Security Hub CSPM untuk mengotomatiskan Security Hub CSPM dengan Amazon. EventBridge Untuk tindakan kustom, jenis acara adalah Security Hub Findings - Custom Action. Setelah menyiapkan tindakan kustom, Anda dapat mengirim temuan ke tindakan tersebut. Untuk informasi selengkapnya dan langkah-langkah terperinci tentang membuat tindakan kustom, lihatthe section called “Respon dan remediasi otomatis”.

Untuk mengirim temuan ke tindakan khusus (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Untuk menampilkan daftar pencarian, lakukan salah satu hal berikut:
   - Di panel navigasi CSPM Hub Keamanan, pilih Temuan.
   - Di panel navigasi CSPM Hub Keamanan, pilih Wawasan. Pilih wawasan. Kemudian pada daftar hasil, pilih hasil wawasan.
   - Di panel navigasi CSPM Hub Keamanan, pilih Integrasi. Pilih Lihat temuan untuk integrasi.

- Di panel navigasi Security Hub CSPM, pilih Standar keamanan. Pilih Lihat hasil untuk menampilkan daftar kontrol. Kemudian pilih nama kontrol.

3. Dalam daftar pencarian, pilih kotak centang untuk setiap temuan yang akan dikirim ke tindakan kustom.

   Anda dapat mengirim hingga 20 temuan sekaligus.

4. Untuk Tind akan, pilih tindakan kustom.

AWS Format Penemuan Keamanan (ASFF)

AWS Security Hub CSPM mengkonsumsi dan mengumpulkan temuan dari produk terintegrasi Layanan AWS dan pihak ketiga. Security Hub CSPM memproses temuan ini menggunakan format temuan standar yang disebut AWS Security Finding Format (ASFF), yang menghilangkan kebutuhan untuk upaya konversi data yang memakan waktu.

Halaman ini memberikan garis besar lengkap JSON untuk temuan dalam Format Penem AWS uan Keamanan (ASFF). Format berasal dari JSON Schema. Pilih nama objek yang ditautkan untuk meninjau contoh penemuan untuk objek itu. Membandingkan temuan CSPM Security Hub Anda dengan sumber daya dan contoh yang ditunjukkan di sini dapat membantu Anda menafsirkan temuan Anda.

Untuk deskripsi atribut ASFF individu, lihat the section called “Atribut ASFF tingkat atas yang diperlukan” danthe section called “Atribut ASFF tingkat atas opsional”.

```
"Findings": [
    {
     "Action": {
      "ActionType": "string",
      "AwsApiCallAction": {
       "AffectedResources": {
        "string": "string"
       },
       "Api": "string",
       "CallerType": "string",
       "DomainDetails": {
        "Domain": "string"
       },
       "FirstSeen": "string",
       "LastSeen": "string",
       "RemoteIpDetails": {
```

```
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
         "Lat": number,
         "Lon": number
        },
        "Organization": {
         "Asn": number,
         "AsnOrg": "string",
         "Isp": "string",
         "Org": "string"
        }
       },
       "ServiceName": "string"
      },
      "DnsRequestAction": {
       "Blocked": boolean,
       "Domain": "string",
       "Protocol": "string"
      },
      "NetworkConnectionAction": {
       "Blocked": boolean,
       "ConnectionDirection": "string",
       "LocalPortDetails": {
        "Port": number,
        "PortName": "string"
       },
       "Protocol": "string",
       "RemoteIpDetails": {
        "City": {
         "CityName": "string"
        },
        "Country": {
         "CountryCode": "string",
         "CountryName": "string"
        },
        "IpAddressV4": "string",
        "Geolocation": {
```

```
          "Lat": number,
          "Lon": number
         },
         "Organization": {
          "Asn": number,
          "AsnOrg": "string",
          "Isp": "string",
          "Org": "string"
         }
        },
        "RemotePortDetails": {
         "Port": number,
         "PortName": "string"
        }
       },
       "PortProbeAction": {
        "Blocked": boolean,
        "PortProbeDetails": [{
         "LocalIpDetails": {
          "IpAddressV4": "string"
         },
         "LocalPortDetails": {
          "Port": number,
          "PortName": "string"
         },
         "RemoteIpDetails": {
          "City": {
           "CityName": "string"
          },
          "Country": {
           "CountryCode": "string",
           "CountryName": "string"
          },
          "GeoLocation": {
           "Lat": number,
           "Lon": number
          },
          "IpAddressV4": "string",
          "Organization": {
           "Asn": number,
           "AsnOrg": "string",
           "Isp": "string",
           "Org": "string"
          }
```

```
        }
       }]
      }
     },
     "AwsAccountId": "string",
     "AwsAccountName": "string",
     "CompanyName": "string",
     "Compliance": {
      "AssociatedStandards": [{
       "StandardsId": "string"
      }],
      "RelatedRequirements": ["string"],
      "SecurityControlId": "string",
      "SecurityControlParameters": [
       {
        "Name": "string",
        "Value": ["string"]
       }
     ],
      "Status": "string",
      "StatusReasons": [
       {
        "Description": "string",
        "ReasonCode": "string"
       }
      ]
     },
     "Confidence": number,
     "CreatedAt": "string",
     "Criticality": number,
     "Description": "string",
     "Detection": {
      "Sequence": {
       "Uid": "string",
       "Actors": [{
        "Id": "string",
        "Session": {
         "Uid": "string",
         "MfAStatus": "string",
         "CreatedTime": "string",
         "Issuer": "string"
        },
        "User": {
         "CredentialUid": "string",
```

```
          "Name": "string",
          "Type": "string",
          "Uid": "string",
          "Account": {
           "Uid": "string",
           "Name": "string"
          }
         }
        }],
        "Endpoints": [{
         "Id": "string",
         "Ip": "string",
         "Domain": "string",
         "Port": number,
         "Location": {
          "City": "string",
          "Country": "string",
          "Lat": number,
          "Lon": number
         },
         "AutonomousSystem": {
          "Name": "string",
          "Number": number
         },
         "Connection": {
          "Direction": "string"
         }
        }],
        "Signals": [{
         "Id": "string",
         "Title": "string",
         "ActorIds": ["string"],
         "Count": number,
         "FirstSeenAt": number,
         "SignalIndicators": [
          {
           "Key": "string",
           "Title": "string",
           "Values": ["string"]
          },
          {
           "Key": "string",
           "Title": "string",
           "Values": ["string"]
```

```
        }
       ],
       "LastSeenAt": number,
       "Name": "string",
       "ResourceIds": ["string"],
       "Type": "string"
      }],
      "SequenceIndicators": [
       {
        "Key": "string",
        "Title": "string",
        "Values": ["string"]
       },
       {
        "Key": "string",
        "Title": "string",
        "Values": ["string"]
       }
      ]
     }
    },
    "FindingProviderFields": {
     "Confidence": number,
     "Criticality": number,
     "RelatedFindings": [{
      "ProductArn": "string",
      "Id": "string"
     }],
     "Severity": {
      "Label": "string",
      "Normalized": number,
      "Original": "string"
     },
     "Types": ["string"]
    },
    "FirstObservedAt": "string",
    "GeneratorId": "string",
    "Id": "string",
    "LastObservedAt": "string",
    "Malware": [{
     "Name": "string",
     "Path": "string",
     "State": "string",
     "Type": "string"
```

```
      }],
      "Network": {
       "DestinationDomain": "string",
       "DestinationIpV4": "string",
       "DestinationIpV6": "string",
       "DestinationPort": number,
       "Direction": "string",
       "OpenPortRange": {
        "Begin": integer,
        "End": integer
       },
       "Protocol": "string",
       "SourceDomain": "string",
       "SourceIpV4": "string",
       "SourceIpV6": "string",
       "SourceMac": "string",
       "SourcePort": number
      },
      "NetworkPath": [{
       "ComponentId": "string",
       "ComponentType": "string",
       "Egress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        },
        "Protocol": "string",
        "Source": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
         }]
        }
       },
       "Ingress": {
        "Destination": {
         "Address": ["string"],
         "PortRanges": [{
          "Begin": integer,
          "End": integer
```

```
        }]
       },
       "Protocol": "string",
       "Source": {
        "Address": ["string"],
        "PortRanges": [{
         "Begin": integer,
         "End": integer
        }]
       }
      }
     }],
     "Note": {
      "Text": "string",
      "UpdatedAt": "string",
      "UpdatedBy": "string"
     },
     "PatchSummary": {
      "FailedCount": number,
      "Id": "string",
      "InstalledCount": number,
      "InstalledOtherCount": number,
      "InstalledPendingReboot": number,
      "InstalledRejectedCount": number,
      "MissingCount": number,
      "Operation": "string",
      "OperationEndTime": "string",
      "OperationStartTime": "string",
      "RebootOption": "string"
     },
     "Process": {
      "LaunchedAt": "string",
      "Name": "string",
      "ParentPid": number,
      "Path": "string",
      "Pid": number,
      "TerminatedAt": "string"
     },
     "ProductArn": "string",
     "ProductFields": {
      "string": "string"
     },
     "ProductName": "string",
     "RecordState": "string",
```

```
      "Region": "string",
      "RelatedFindings": [{
       "Id": "string",
       "ProductArn": "string"
      }],
      "Remediation": {
       "Recommendation": {
        "Text": "string",
        "Url": "string"
       }
      },
      "Resources": [{
       "ApplicationArn": "string",
       "ApplicationName": "string",
       "DataClassification": {
        "DetailedResultsLocation": "string",
        "Result": {
         "AdditionalOccurrences": boolean,
         "CustomDataIdentifiers": {
          "Detections": [{
           "Arn": "string",
           "Count": integer,
           "Name": "string",
           "Occurrences": {
            "Cells": [{
             "CellReference": "string",
             "Column": integer,
             "ColumnName": "string",
             "Row": integer
            }],
            "LineRanges": [{
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            }],
            "OffsetRanges": [{
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            }],
            "Pages": [{
             "LineRange": {
              "End": integer,
              "Start": integer,
```

```
            "StartColumn": integer
           },
           "OffsetRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
           },
           "PageNumber": integer
          }],
          "Records": [{
           "JsonPath": "string",
           "RecordIndex": integer
          }]
         }
        }],
        "TotalCount": integer
       },
       "MimeType": "string",
       "SensitiveData": [{
        "Category": "string",
        "Detections": [{
         "Count": integer,
         "Occurrences": {
          "Cells": [{
           "CellReference": "string",
           "Column": integer,
           "ColumnName": "string",
           "Row": integer
          }],
          "LineRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "OffsetRanges": [{
           "End": integer,
           "Start": integer,
           "StartColumn": integer
          }],
          "Pages": [{
           "LineRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
```

```
            },
            "OffsetRange": {
             "End": integer,
             "Start": integer,
             "StartColumn": integer
            },
            "PageNumber": integer
           }],
           "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
           }]
          },
          "Type": "string"
         }],
         "TotalCount": integer
        }],
        "SizeClassified": integer,
        "Status": {
         "Code": "string",
         "Reason": "string"
        }
       }
      },
      "Details": {
       "AwsAmazonMQBroker": {
        "AutoMinorVersionUpgrade": boolean,
        "BrokerArn": "string",
        "BrokerId": "string",
        "BrokerName": "string",
        "Configuration": {
         "Id": "string",
         "Revision": integer
        },
        "DeploymentMode": "string",
        "EncryptionOptions": {
         "UseAwsOwnedKey": boolean
        },
        "EngineType": "string",
        "EngineVersion": "string",
        "HostInstanceType": "string",
        "Logs": {
         "Audit": boolean,
         "AuditLogGroup": "string",
```

```
          "General": boolean,
          "GeneralLogGroup": "string"
         },
         "MaintenanceWindowStartTime": {
          "DayOfWeek": "string",
          "TimeOfDay": "string",
          "TimeZone": "string"
         },
         "PubliclyAccessible": boolean,
         "SecurityGroups": [
          "string"
         ],
         "StorageType": "string",
         "SubnetIds": [
          "string",
          "string"
         ],
         "Users": [{
          "Username": "string"
         }]
        },
        "AwsApiGatewayRestApi": {
         "ApiKeySource": "string",
         "BinaryMediaTypes": [" string"],
         "CreatedDate": "string",
         "Description": "string",
         "EndpointConfiguration": {
          "Types": ["string"]
         },
         "Id": "string",
         "MinimumCompressionSize": number,
         "Name": "string",
         "Version": "string"
        },
        "AwsApiGatewayStage": {
         "AccessLogSettings": {
          "DestinationArn": "string",
          "Format": "string"
         },
         "CacheClusterEnabled": boolean,
         "CacheClusterSize": "string",
         "CacheClusterStatus": "string",
         "CanarySettings": {
          "DeploymentId": "string",
```

```
          "PercentTraffic": number,
          "StageVariableOverrides": [{
           "string": "string"
          }],
          "UseStageCache": boolean
         },
         "ClientCertificateId": "string",
         "CreatedDate": "string",
         "DeploymentId": "string",
         "Description": "string",
         "DocumentationVersion": "string",
         "LastUpdatedDate": "string",
         "MethodSettings": [{
          "CacheDataEncrypted": boolean,
          "CachingEnabled": boolean,
          "CacheTtlInSeconds": number,
          "DataTraceEnabled": boolean,
          "HttpMethod": "string",
          "LoggingLevel": "string",
          "MetricsEnabled": boolean,
          "RequireAuthorizationForCacheControl": boolean,
          "ResourcePath": "string",
          "ThrottlingBurstLimit": number,
          "ThrottlingRateLimit": number,
          "UnauthorizedCacheControlHeaderStrategy": "string"
         }],
         "StageName": "string",
         "TracingEnabled": boolean,
         "Variables": {
          "string": "string"
         },
         "WebAclArn": "string"
        },
        "AwsApiGatewayV2Api": {
         "ApiEndpoint": "string",
         "ApiId": "string",
         "ApiKeySelectionExpression": "string",
         "CorsConfiguration": {
          "AllowCredentials": boolean,
          "AllowHeaders": ["string"],
          "AllowMethods": ["string"],
          "AllowOrigins": ["string"],
          "ExposeHeaders": ["string"],
          "MaxAge": number
```

```
        },
        "CreatedDate": "string",
        "Description": "string",
        "Name": "string",
        "ProtocolType": "string",
        "RouteSelectionExpression": "string",
        "Version": "string"
       },
       "AwsApiGatewayV2Stage": {
        "AccessLogSettings": {
         "DestinationArn": "string",
         "Format": "string"
        },
        "ApiGatewayManaged": boolean,
        "AutoDeploy": boolean,
        "ClientCertificateId": "string",
        "CreatedDate": "string",
        "DefaultRouteSettings": {
         "DataTraceEnabled": boolean,
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "DeploymentId": "string",
        "Description": "string",
        "LastDeploymentStatusMessage": "string",
        "LastUpdatedDate": "string",
        "RouteSettings": {
         "DetailedMetricsEnabled": boolean,
         "LoggingLevel": "string",
         "DataTraceEnabled": boolean,
         "ThrottlingBurstLimit": number,
         "ThrottlingRateLimit": number
        },
        "StageName": "string",
        "StageVariables": [{
         "string": "string"
        }]
       },
       "AwsAppSyncGraphQLApi": {
        "AwsAppSyncGraphQlApi": {
         "AdditionalAuthenticationProviders": [
         {
```

```
          "AuthenticationType": "string",
          "LambdaAuthorizerConfig": {
           "AuthorizerResultTtlInSeconds": integer,
           "AuthorizerUri": "string"
          }
         },
         {
          "AuthenticationType": "string"
         }
         ],
         "ApiId": "string",
         "Arn": "string",
         "AuthenticationType": "string",
         "Id": "string",
         "LogConfig": {
          "CloudWatchLogsRoleArn": "string",
          "ExcludeVerboseContent": boolean,
          "FieldLogLevel": "string"
         },
         "Name": "string",
         "XrayEnabled": boolean
        }
       },
       "AwsAthenaWorkGroup": {
        "Description": "string",
        "Name": "string",
        "WorkgroupConfiguration": {
         "ResultConfiguration": {
          "EncryptionConfiguration": {
           "EncryptionOption": "string",
           "KmsKey": "string"
          }
         }
        },
        "State": "string"
       },
       "AwsAutoScalingAutoScalingGroup": {
        "AvailabilityZones": [{
         "Value": "string"
        }],
        "CreatedTime": "string",
        "HealthCheckGracePeriod": integer,
        "HealthCheckType": "string",
        "LaunchConfigurationName": "string",
```

```
        "LoadBalancerNames": ["string"],
        "LaunchTemplate": {
                        "LaunchTemplateId": "string",
                        "LaunchTemplateName": "string",
                        "Version": "string"
                    },
        "MixedInstancesPolicy": {
         "InstancesDistribution": {
          "OnDemandAllocationStrategy": "string",
          "OnDemandBaseCapacity": number,
          "OnDemandPercentageAboveBaseCapacity": number,
          "SpotAllocationStrategy": "string",
          "SpotInstancePools": number,
          "SpotMaxPrice": "string"
         },
         "LaunchTemplate": {
          "LaunchTemplateSpecification": {
           "LaunchTemplateId": "string",
           "LaunchTemplateName": "string",
           "Version": "string"
          },
          "CapacityRebalance": boolean,
          "Overrides": [{
           "InstanceType": "string",
           "WeightedCapacity": "string"
          }]
         }
        },
        "AwsAutoScalingLaunchConfiguration": {
         "AssociatePublicIpAddress": boolean,
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteOnTermination": boolean,
           "Encrypted": boolean,
           "Iops": number,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          },
          "NoDevice": boolean,
          "VirtualName": "string"
         }],
```

```
        "ClassicLinkVpcId": "string",
        "ClassicLinkVpcSecurityGroups": ["string"],
        "CreatedTime": "string",
        "EbsOptimized": boolean,
        "IamInstanceProfile": "string"
       },
       "ImageId": "string",
       "InstanceMonitoring": {
        "Enabled": boolean
       },
       "InstanceType": "string",
       "KernelId": "string",
       "KeyName": "string",
       "LaunchConfigurationName": "string",
       "MetadataOptions": {
        "HttpEndPoint": "string",
        "HttpPutReponseHopLimit": number,
        "HttpTokens": "string"
       },
       "PlacementTenancy": "string",
       "RamdiskId": "string",
       "SecurityGroups": ["string"],
       "SpotPrice": "string",
       "UserData": "string"
      },
      "AwsBackupBackupPlan": {
       "BackupPlan": {
        "AdvancedBackupSettings": [{
         "BackupOptions": {
          "WindowsVSS":"string"
         },
         "ResourceType":"string"
        }],
        "BackupPlanName": "string",
        "BackupPlanRule": [{
         "CompletionWindowMinutes": integer,
         "CopyActions": [{
          "DestinationBackupVaultArn": "string",
          "Lifecycle": {
           "DeleteAfterDays": integer,
           "MoveToColdStorageAfterDays": integer
          }
         }],
         "Lifecycle": {
```

```
          "DeleteAfterDays": integer
         },
         "RuleName": "string",
         "ScheduleExpression": "string",
         "StartWindowMinutes": integer,
         "TargetBackupVault": "string"
        }]
       },
       "BackupPlanArn": "string",
       "BackupPlanId": "string",
       "VersionId": "string"
     },
      "AwsBackupBackupVault": {
       "AccessPolicy": {
        "Statement": [{
         "Action": ["string"],
         "Effect": "string",
         "Principal": {
          "AWS": "string"
         },
         "Resource": "string"
        }],
        "Version": "string"
       },
       "BackupVaultArn": "string",
       "BackupVaultName": "string",
       "EncryptionKeyArn": "string",
       "Notifications": {
        "BackupVaultEvents": ["string"],
        "SNSTopicArn": "string"
       }
      },
      "AwsBackupRecoveryPoint": {
       "BackupSizeInBytes": integer,
       "BackupVaultName": "string",
       "BackupVaultArn": "string",
       "CalculatedLifecycle": {
        "DeleteAt": "string",
        "MoveToColdStorageAt": "string"
       },
       "CompletionDate": "string",
       "CreatedBy": {
        "BackupPlanArn": "string",
        "BackupPlanId": "string",
```

```
        "BackupPlanVersion": "string",
        "BackupRuleId": "string"
       },
       "CreationDate": "string",
       "EncryptionKeyArn": "string",
       "IamRoleArn": "string",
       "IsEncrypted": boolean,
       "LastRestoreTime": "string",
       "Lifecycle": {
        "DeleteAfterDays": integer,
        "MoveToColdStorageAfterDays": integer
       },
       "RecoveryPointArn": "string",
       "ResourceArn": "string",
       "ResourceType": "string",
       "SourceBackupVaultArn": "string",
       "Status": "string",
       "StatusMessage": "string",
       "StorageClass": "string"
      },
      "AwsCertificateManagerCertificate": {
       "CertificateAuthorityArn": "string",
       "CreatedAt": "string",
       "DomainName": "string",
       "DomainValidationOptions": [{
        "DomainName": "string",
        "ResourceRecord": {
         "Name": "string",
         "Type": "string",
         "Value": "string"
        },
        "ValidationDomain": "string",
        "ValidationEmails": ["string"],
        "ValidationMethod": "string",
        "ValidationStatus": "string"
       }],
       "ExtendedKeyUsages": [{
        "Name": "string",
        "OId": "string"
       }],
       "FailureReason": "string",
       "ImportedAt": "string",
       "InUseBy": ["string"],
       "IssuedAt": "string",
```

```
        "Issuer": "string",
        "KeyAlgorithm": "string",
        "KeyUsages": [{
         "Name": "string"
        }],
        "NotAfter": "string",
        "NotBefore": "string",
        "Options": {
         "CertificateTransparencyLoggingPreference": "string"
        },
        "RenewalEligibility": "string",
        "RenewalSummary": {
         "DomainValidationOptions": [{
          "DomainName": "string",
          "ResourceRecord": {
           "Name": "string",
           "Type": "string",
           "Value": "string"
          },
          "ValidationDomain": "string",
          "ValidationEmails": ["string"],
          "ValidationMethod": "string",
          "ValidationStatus": "string"
         }],
         "RenewalStatus": "string",
         "RenewalStatusReason": "string",
         "UpdatedAt": "string"
        },
        "Serial": "string",
        "SignatureAlgorithm": "string",
        "Status": "string",
        "Subject": "string",
        "SubjectAlternativeNames": ["string"],
        "Type": "string"
       },
       "AwsCloudFormationStack": {
        "Capabilities": ["string"],
        "CreationTime": "string",
        "Description": "string",
        "DisableRollback": boolean,
        "DriftInformation": {
         "StackDriftStatus": "string"
        },
        "EnableTerminationProtection": boolean,
```

```
        "LastUpdatedTime": "string",
        "NotificationArns": ["string"],
        "Outputs": [{
         "Description": "string",
         "OutputKey": "string",
         "OutputValue": "string"
        }],
        "RoleArn": "string",
        "StackId": "string",
        "StackName": "string",
        "StackStatus": "string",
        "StackStatusReason": "string",
        "TimeoutInMinutes": number
       },
       "AwsCloudFrontDistribution": {
        "CacheBehaviors": {
         "Items": [{
          "ViewerProtocolPolicy": "string"
         }]
        },
        "DefaultCacheBehavior": {
         "ViewerProtocolPolicy": "string"
        },
        "DefaultRootObject": "string",
        "DomainName": "string",
        "Etag": "string",
        "LastModifiedTime": "string",
        "Logging": {
         "Bucket": "string",
         "Enabled": boolean,
         "IncludeCookies": boolean,
         "Prefix": "string"
        },
        "OriginGroups": {
         "Items": [{
          "FailoverCriteria": {
           "StatusCodes": {
            "Items": [number],
            "Quantity": number
           }
          }
         }]
        },
        "Origins": {
```

```
        "Items": [{
         "CustomOriginConfig": {
          "HttpPort": number,
          "HttpsPort": number,
          "OriginKeepaliveTimeout": number,
          "OriginProtocolPolicy": "string",
          "OriginReadTimeout": number,
          "OriginSslProtocols": {
           "Items": ["string"],
           "Quantity": number
          }
         },
         "DomainName": "string",
         "Id": "string",
         "OriginPath": "string",
         "S3OriginConfig": {
          "OriginAccessIdentity": "string"
         }
        }]
       },
       "Status": "string",
       "ViewerCertificate": {
        "AcmCertificateArn": "string",
        "Certificate": "string",
        "CertificateSource": "string",
        "CloudFrontDefaultCertificate": boolean,
        "IamCertificateId": "string",
        "MinimumProtocolVersion": "string",
        "SslSupportMethod": "string"
       },
       "WebAclId": "string"
      },
      "AwsCloudTrailTrail": {
       "CloudWatchLogsLogGroupArn": "string",
       "CloudWatchLogsRoleArn": "string",
       "HasCustomEventSelectors": boolean,
       "HomeRegion": "string",
       "IncludeGlobalServiceEvents": boolean,
       "IsMultiRegionTrail": boolean,
       "IsOrganizationTrail": boolean,
       "KmsKeyId": "string",
       "LogFileValidationEnabled": boolean,
       "Name": "string",
       "S3BucketName": "string",
```

```
        "S3KeyPrefix": "string",
        "SnsTopicArn": "string",
        "SnsTopicName": "string",
        "TrailArn": "string"
       },
       "AwsCloudWatchAlarm": {
        "ActionsEnabled": boolean,
        "AlarmActions": ["string"],
        "AlarmArn": "string",
        "AlarmConfigurationUpdatedTimestamp": "string",
        "AlarmDescription": "string",
        "AlarmName": "string",
        "ComparisonOperator": "string",
        "DatapointsToAlarm": number,
        "Dimensions": [{
         "Name": "string",
         "Value": "string"
        }],
        "EvaluateLowSampleCountPercentile": "string",
        "EvaluationPeriods": number,
        "ExtendedStatistic": "string",
        "InsufficientDataActions": ["string"],
        "MetricName": "string",
        "Namespace": "string",
        "OkActions": ["string"],
        "Period": number,
        "Statistic": "string",
        "Threshold": number,
        "ThresholdMetricId": "string",
        "TreatMissingData": "string",
        "Unit": "string"
       },
       "AwsCodeBuildProject": {
        "Artifacts": [{
         "ArtifactIdentifier": "string",
         "EncryptionDisabled": boolean,
         "Location": "string",
         "Name": "string",
         "NamespaceType": "string",
         "OverrideArtifactName": boolean,
         "Packaging": "string",
         "Path": "string",
         "Type": "string"
        }],
```

```
        "SecondaryArtifacts": [{
                    "ArtifactIdentifier": "string",
                    "Type": "string",
                    "Location": "string",
                    "Name": "string",
                    "NamespaceType": "string",
                    "Packaging": "string",
                    "Path": "string",
                    "EncryptionDisabled": boolean,
                    "OverrideArtifactName": boolean
                }],
        "EncryptionKey": "string",
        "Certificate": "string",
        "Environment": {
         "Certificate": "string",
         "EnvironmentVariables": [{
          "Name": "string",
          "Type": "string",
          "Value": "string"
         }],
         "ImagePullCredentialsType": "string",
         "PrivilegedMode": boolean,
         "RegistryCredential": {
          "Credential": "string",
          "CredentialProvider": "string"
         },
         "Type": "string"
        },
        "LogsConfig": {
         "CloudWatchLogs": {
          "GroupName": "string",
          "Status": "string",
          "StreamName": "string"
         },
         "S3Logs": {
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Status": "string"
         }
        },
        "Name": "string",
        "ServiceRole": "string",
        "Source": {
         "Type": "string",
```

```
        "Location": "string",
        "GitCloneDepth": integer
      },
      "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
      }
    },
    "AwsDmsEndpoint": {
      "CertificateArn": "string",
      "DatabaseName": "string",
      "EndpointArn": "string",
      "EndpointIdentifier": "string",
      "EndpointType": "string",
      "EngineName": "string",
      "KmsKeyId": "string",
      "Port": integer,
      "ServerName": "string",
      "SslMode": "string",
      "Username": "string"
    },
    "AwsDmsReplicationInstance": {
      "AllocatedStorage": integer,
      "AutoMinorVersionUpgrade": boolean,
      "AvailabilityZone": "string",
      "EngineVersion": "string",
      "KmsKeyId": "string",
      "MultiAZ": boolean,
      "PreferredMaintenanceWindow": "string",
      "PubliclyAccessible": boolean,
      "ReplicationInstanceClass": "string",
      "ReplicationInstanceIdentifier": "string",
      "ReplicationSubnetGroup": {
          "ReplicationSubnetGroupIdentifier": "string"
      },
      "VpcSecurityGroups": [
          {
              "VpcSecurityGroupId": "string"
          }
      ]
    },
    "AwsDmsReplicationTask": {
      "CdcStartPosition": "string",
```

```
        "Id": "string",
        "MigrationType": "string",
        "ReplicationInstanceArn": "string",
        "ReplicationTaskIdentifier": "string",
        "ReplicationTaskSettings": {
         "string": "string"
        },
        "SourceEndpointArn": "string",
        "TableMappings": {
         "string": "string"
        },
        "TargetEndpointArn": "string"
       },
       "AwsDynamoDbTable": {
        "AttributeDefinitions": [{
         "AttributeName": "string",
         "AttributeType": "string"
        }],
        "BillingModeSummary": {
         "BillingMode": "string",
         "LastUpdateToPayPerRequestDateTime": "string"
        },
        "CreationDateTime": "string",
        "DeletionProtectionEnabled": boolean,
        "GlobalSecondaryIndexes": [{
         "Backfilling": boolean,
         "IndexArn": "string",
         "IndexName": "string",
         "IndexSizeBytes": number,
         "IndexStatus": "string",
         "ItemCount": number,
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         },
         "ProvisionedThroughput": {
          "LastDecreaseDateTime": "string",
          "LastIncreaseDateTime": "string",
          "NumberOfDecreasesToday": number,
          "ReadCapacityUnits": number,
```

```
          "WriteCapacityUnits": number
         }
        }],
        "GlobalTableVersion": "string",
        "ItemCount": number,
        "KeySchema": [{
         "AttributeName": "string",
         "KeyType": "string"
        }],
        "LatestStreamArn": "string",
        "LatestStreamLabel": "string",
        "LocalSecondaryIndexes": [{
         "IndexArn": "string",
         "IndexName": "string",
         "KeySchema": [{
          "AttributeName": "string",
          "KeyType": "string"
         }],
         "Projection": {
          "NonKeyAttributes": ["string"],
          "ProjectionType": "string"
         }
        }],
        "ProvisionedThroughput": {
         "LastDecreaseDateTime": "string",
         "LastIncreaseDateTime": "string",
         "NumberOfDecreasesToday": number,
         "ReadCapacityUnits": number,
         "WriteCapacityUnits": number
        },
        "Replicas": [{
         "GlobalSecondaryIndexes": [{
          "IndexName": "string",
          "ProvisionedThroughputOverride": {
           "ReadCapacityUnits": number
          }
         }],
         "KmsMasterKeyId": "string",
         "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": number
         },
         "RegionName": "string",
         "ReplicaStatus": "string",
         "ReplicaStatusDescription": "string"
```

```
        }],
        "RestoreSummary": {
         "RestoreDateTime": "string",
         "RestoreInProgress": boolean,
         "SourceBackupArn": "string",
         "SourceTableArn": "string"
        },
        "SseDescription": {
         "InaccessibleEncryptionDateTime": "string",
         "KmsMasterKeyArn": "string",
         "SseType": "string",
         "Status": "string"
        },
        "StreamSpecification": {
         "StreamEnabled": boolean,
         "StreamViewType": "string"
        },
        "TableId": "string",
        "TableName": "string",
        "TableSizeBytes": number,
        "TableStatus": "string"
       },
       "AwsEc2ClientVpnEndpoint": {
        "AuthenticationOptions": [
         {
          "MutualAuthentication": {
           "ClientRootCertificateChainArn": "string"
          },
          "Type": "string"
         }
        ],
        "ClientCidrBlock": "string",
        "ClientConnectOptions": {
         "Enabled": boolean
        },
        "ClientLoginBannerOptions": {
         "Enabled": boolean
        },
        "ClientVpnEndpointId": "string",
        "ConnectionLogOptions": {
         "Enabled": boolean
        },
        "Description": "string",
        "DnsServer": ["string"],
```

```
        "ServerCertificateArn": "string",
        "SecurityGroupIdSet": [
         "string"
        ],
        "SelfServicePortalUrl": "string",
        "SessionTimeoutHours": "integer",
        "SplitTunnel": boolean,
        "TransportProtocol": "string",
        "VpcId": "string",
        "VpnPort": integer
       },
       "AwsEc2Eip": {
        "AllocationId": "string",
        "AssociationId": "string",
        "Domain": "string",
        "InstanceId": "string",
        "NetworkBorderGroup": "string",
        "NetworkInterfaceId": "string",
        "NetworkInterfaceOwnerId": "string",
        "PrivateIpAddress": "string",
        "PublicIp": "string",
        "PublicIpv4Pool": "string"
       },
       "AwsEc2Instance": {
        "IamInstanceProfileArn": "string",
        "ImageId": "string",
        "IpV4Addresses": ["string"],
        "IpV6Addresses": ["string"],
        "KeyName": "string",
        "LaunchedAt": "string",
        "MetadataOptions": {
         "HttpEndpoint": "string",
         "HttpProtocolIpv6": "string",
         "HttpPutResponseHopLimit": number,
         "HttpTokens": "string",
         "InstanceMetadataTags": "string"
        },
        "Monitoring": {
         "State": "string"
        },
        "NetworkInterfaces": [{
         "NetworkInterfaceId": "string"
        }],
        "SubnetId": "string",
```

```
        "Type": "string",
        "VirtualizationType": "string",
        "VpcId": "string"
       },
       "AwsEc2LaunchTemplate": {
        "DefaultVersionNumber": "string",
        "ElasticGpuSpecifications": ["string"],
        "ElasticInferenceAccelerators": ["string"],
        "Id": "string",
        "ImageId": "string",
        "LatestVersionNumber": "string",
        "LaunchTemplateData": {
         "BlockDeviceMappings": [{
          "DeviceName": "string",
          "Ebs": {
           "DeleteonTermination": boolean,
           "Encrypted": boolean,
           "SnapshotId": "string",
           "VolumeSize": number,
           "VolumeType": "string"
          }
         }],
         "MetadataOptions": {
          "HttpTokens": "string",
          "HttpPutResponseHopLimit" : number
         },
         "Monitoring": {
          "Enabled": boolean
         },
         "NetworkInterfaces": [{
          "AssociatePublicIpAddress" : boolean
         }]
        },
        "LaunchTemplateName": "string",
        "LicenseSpecifications": ["string"],
        "SecurityGroupIds": ["string"],
        "SecurityGroups": ["string"],
        "TagSpecifications": ["string"]
       },
       "AwsEc2NetworkAcl": {
        "Associations": [{
         "NetworkAclAssociationId": "string",
         "NetworkAclId": "string",
         "SubnetId": "string"
```

```
        }],
        "Entries": [{
         "CidrBlock": "string",
         "Egress": boolean,
         "IcmpTypeCode": {
          "Code": number,
          "Type": number
         },
         "Ipv6CidrBlock": "string",
         "PortRange": {
          "From": number,
          "To": number
         },
         "Protocol": "string",
         "RuleAction": "string",
         "RuleNumber": number
        }],
        "IsDefault": boolean,
        "NetworkAclId": "string",
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2NetworkInterface": {
        "Attachment": {
         "AttachmentId": "string",
         "AttachTime": "string",
         "DeleteOnTermination": boolean,
         "DeviceIndex": number,
         "InstanceId": "string",
         "InstanceOwnerId": "string",
         "Status": "string"
        },
        "Ipv6Addresses": [{
         "Ipv6Address": "string"
        }],
        "NetworkInterfaceId": "string",
        "PrivateIpAddresses": [{
         "PrivateDnsName": "string",
         "PrivateIpAddress": "string"
        }],
        "PublicDnsName": "string",
        "PublicIp": "string",
        "SecurityGroups": [{
         "GroupId": "string",
```

```
        "GroupName": "string"
       }],
       "SourceDestCheck": boolean
      },
      "AwsEc2RouteTable": {
       "AssociationSet": [{
        "AssociationState": {
         "State": "string"
        },
        "Main": boolean,
        "RouteTableAssociationId": "string",
        "RouteTableId": "string"
       }],
       "PropogatingVgwSet": [],
       "RouteTableId": "string",
       "RouteSet": [
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        },
        {
         "DestinationCidrBlock": "string",
         "GatewayId": "string",
         "Origin": "string",
         "State": "string"
        }
       ],
       "VpcId": "string"
      },
      "AwsEc2SecurityGroup": {
       "GroupId": "string",
       "GroupName": "string",
       "IpPermissions": [{
        "FromPort": number,
        "IpProtocol": "string",
        "IpRanges": [{
         "CidrIp": "string"
        }],
        "Ipv6Ranges": [{
         "CidrIpv6": "string"
        }],
        "PrefixListIds": [{
```

```
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "IpPermissionsEgress": [{
         "FromPort": number,
         "IpProtocol": "string",
         "IpRanges": [{
          "CidrIp": "string"
         }],
         "Ipv6Ranges": [{
          "CidrIpv6": "string"
         }],
         "PrefixListIds": [{
          "PrefixListId": "string"
         }],
         "ToPort": number,
         "UserIdGroupPairs": [{
          "GroupId": "string",
          "GroupName": "string",
          "PeeringStatus": "string",
          "UserId": "string",
          "VpcId": "string",
          "VpcPeeringConnectionId": "string"
         }]
        }],
        "OwnerId": "string",
        "VpcId": "string"
       },
       "AwsEc2Subnet": {
        "AssignIpv6AddressOnCreation": boolean,
        "AvailabilityZone": "string",
        "AvailabilityZoneId": "string",
        "AvailableIpAddressCount": number,
        "CidrBlock": "string",
        "DefaultForAz": boolean,
```

```
        "Ipv6CidrBlockAssociationSet": [{
         "AssociationId": "string",
         "Ipv6CidrBlock": "string",
         "CidrBlockState": "string"
        }],
        "MapPublicIpOnLaunch": boolean,
        "OwnerId": "string",
        "State": "string",
        "SubnetArn": "string",
        "SubnetId": "string",
        "VpcId": "string"
       },
       "AwsEc2TransitGateway": {
        "AmazonSideAsn": number,
        "AssociationDefaultRouteTableId": "string",
        "AutoAcceptSharedAttachments": "string",
        "DefaultRouteTableAssociation": "string",
        "DefaultRouteTablePropagation": "string",
        "Description": "string",
        "DnsSupport": "string",
        "Id": "string",
        "MulticastSupport": "string",
        "PropagationDefaultRouteTableId": "string",
        "TransitGatewayCidrBlocks": ["string"],
        "VpnEcmpSupport": "string"
       },
       "AwsEc2Volume": {
        "Attachments": [{
         "AttachTime": "string",
         "DeleteOnTermination": boolean,
         "InstanceId": "string",
         "Status": "string"
        }],
        "CreateTime": "string",
        "DeviceName": "string",
        "Encrypted": boolean,
        "KmsKeyId": "string",
        "Size": number,
        "SnapshotId": "string",
        "Status": "string",
        "VolumeId": "string",
        "VolumeScanStatus": "string",
        "VolumeType": "string"
       },
```

```
      "AwsEc2Vpc": {
       "CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlock": "string",
        "CidrBlockState": "string"
       }],
       "DhcpOptionsId": "string",
       "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "string",
        "CidrBlockState": "string",
        "Ipv6CidrBlock": "string"
       }],
       "State": "string"
      },
      "AwsEc2VpcEndpointService": {
       "AcceptanceRequired": boolean,
       "AvailabilityZones": ["string"],
       "BaseEndpointDnsNames": ["string"],
       "ManagesVpcEndpoints": boolean,
       "GatewayLoadBalancerArns": ["string"],
       "NetworkLoadBalancerArns": ["string"],
       "PrivateDnsName": "string",
       "ServiceId": "string",
       "ServiceName": "string",
       "ServiceState": "string",
       "ServiceType": [{
        "ServiceType": "string"
       }]
      },
      "AwsEc2VpcPeeringConnection": {
       "AccepterVpcInfo": {
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
```

```
        "Region": "string",
        "VpcId": "string"
       },
       "ExpirationTime": "string",
       "RequesterVpcInfo": {
        "CidrBlock": "string",
        "CidrBlockSet": [{
         "CidrBlock": "string"
        }],
        "Ipv6CidrBlockSet": [{
         "Ipv6CidrBlock": "string"
        }],
        "OwnerId": "string",
        "PeeringOptions": {
         "AllowDnsResolutionFromRemoteVpc": boolean,
         "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
         "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
        },
        "Region": "string",
        "VpcId": "string"
       },
       "Status": {
        "Code": "string",
        "Message": "string"
       },
       "VpcPeeringConnectionId": "string"
      },
      "AwsEcrContainerImage": {
       "Architecture": "string",
       "ImageDigest": "string",
       "ImagePublishedAt": "string",
       "ImageTags": ["string"],
       "RegistryId": "string",
       "RepositoryName": "string"
      },
      "AwsEcrRepository": {
       "Arn": "string",
       "ImageScanningConfiguration": {
        "ScanOnPush": boolean
       },
       "ImageTagMutability": "string",
       "LifecyclePolicy": {
        "LifecyclePolicyText": "string",
        "RegistryId": "string"
```

```
        },
        "RepositoryName": "string",
        "RepositoryPolicyText": "string"
      },
      "AwsEcsCluster": {
        "ActiveServicesCount": number,
        "CapacityProviders": ["string"],
        "ClusterArn": "string",
        "ClusterName": "string",
        "ClusterSettings": [{
          "Name": "string",
          "Value": "string"
        }],
        "Configuration": {
          "ExecuteCommandConfiguration": {
            "KmsKeyId": "string",
            "LogConfiguration": {
              "CloudWatchEncryptionEnabled": boolean,
              "CloudWatchLogGroupName": "string",
              "S3BucketName": "string",
              "S3EncryptionEnabled": boolean,
              "S3KeyPrefix": "string"
            },
            "Logging": "string"
          }
        },
        "DefaultCapacityProviderStrategy": [{
          "Base": number,
          "CapacityProvider": "string",
          "Weight": number
        }],
        "RegisteredContainerInstancesCount": number,
        "RunningTasksCount": number,
        "Status": "string"
      },
      "AwsEcsContainer": {
        "Image": "string",
        "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
        }],
        "Name": "string",
        "Privileged": boolean
      },
```

```
      "AwsEcsService": {
       "CapacityProviderStrategy": [{
        "Base": number,
        "CapacityProvider": "string",
        "Weight": number
       }],
       "Cluster": "string",
       "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
         "Enable": boolean,
         "Rollback": boolean
        },
        "MaximumPercent": number,
        "MinimumHealthyPercent": number
       },
       "DeploymentController": {
        "Type": "string"
       },
       "DesiredCount": number,
       "EnableEcsManagedTags": boolean,
       "EnableExecuteCommand": boolean,
       "HealthCheckGracePeriodSeconds": number,
       "LaunchType": "string",
       "LoadBalancers": [{
        "ContainerName": "string",
        "ContainerPort": number,
        "LoadBalancerName": "string",
        "TargetGroupArn": "string"
       }],
       "Name": "string",
       "NetworkConfiguration": {
        "AwsVpcConfiguration": {
         "AssignPublicIp": "string",
         "SecurityGroups": ["string"],
         "Subnets": ["string"]
        }
       },
       "PlacementConstraints": [{
        "Expression": "string",
        "Type": "string"
       }],
       "PlacementStrategies": [{
        "Field": "string",
        "Type": "string"
```

```
        }],
        "PlatformVersion": "string",
        "PropagateTags": "string",
        "Role": "string",
        "SchedulingStrategy": "string",
        "ServiceArn": "string",
        "ServiceName": "string",
        "ServiceRegistries": [{
         "ContainerName": "string",
         "ContainerPort": number,
         "Port": number,
         "RegistryArn": "string"
        }],
        "TaskDefinition": "string"
       },
       "AwsEcsTask": {
        "CreatedAt": "string",
        "ClusterArn": "string",
        "Group": "string",
        "StartedAt": "string",
        "StartedBy": "string",
        "TaskDefinitionArn": "string",
        "Version": number,
        "Volumes": [{
         "Name": "string",
         "Host": {
          "SourcePath": "string"
         }
        }],
        "Containers": [{
         "Image": "string",
         "MountPoints": [{
          "ContainerPath": "string",
          "SourceVolume": "string"
         }],
         "Name": "string",
         "Privileged": boolean
        }]
       },
       "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [{
         "Command": ["string"],
         "Cpu": number,
         "DependsOn": [{
```

```
          "Condition": "string",
          "ContainerName": "string"
        }],
        "DisableNetworking": boolean,
        "DnsSearchDomains": ["string"],
        "DnsServers": ["string"],
        "DockerLabels": {
          "string": "string"
        },
        "DockerSecurityOptions": ["string"],
        "EntryPoint": ["string"],
        "Environment": [{
          "Name": "string",
          "Value": "string"
        }],
        "EnvironmentFiles": [{
          "Type": "string",
          "Value": "string"
        }],
        "Essential": boolean,
        "ExtraHosts": [{
          "Hostname": "string",
          "IpAddress": "string"
        }],
        "FirelensConfiguration": {
          "Options": {
            "string": "string"
          },
          "Type": "string"
        },
        "HealthCheck": {
          "Command": ["string"],
          "Interval": number,
          "Retries": number,
          "StartPeriod": number,
          "Timeout": number
        },
        "Hostname": "string",
        "Image": "string",
        "Interactive": boolean,
        "Links": ["string"],
        "LinuxParameters": {
          "Capabilities": {
            "Add": ["string"],
```

```
          "Drop": ["string"]
         },
         "Devices": [{
          "ContainerPath": "string",
          "HostPath": "string",
          "Permissions": ["string"]
         }],
         "InitProcessEnabled": boolean,
         "MaxSwap": number,
         "SharedMemorySize": number,
         "Swappiness": number,
         "Tmpfs": [{
          "ContainerPath": "string",
          "MountOptions": ["string"],
          "Size": number
         }]
        },
        "LogConfiguration": {
         "LogDriver": "string",
         "Options": {
          "string": "string"
         },
         "SecretOptions": [{
          "Name": "string",
          "ValueFrom": "string"
         }]
        },
        "Memory": number,
        "MemoryReservation": number,
        "MountPoints": [{
         "ContainerPath": "string",
         "ReadOnly": boolean,
         "SourceVolume": "string"
        }],
        "Name": "string",
        "PortMappings": [{
         "ContainerPort": number,
         "HostPort": number,
         "Protocol": "string"
        }],
        "Privileged": boolean,
        "PseudoTerminal": boolean,
        "ReadonlyRootFilesystem": boolean,
        "RepositoryCredentials": {
```

```
          "CredentialsParameter": "string"
         },
         "ResourceRequirements": [{
          "Type": "string",
          "Value": "string"
         }],
         "Secrets": [{
          "Name": "string",
          "ValueFrom": "string"
         }],
         "StartTimeout": number,
         "StopTimeout": number,
         "SystemControls": [{
          "Namespace": "string",
          "Value": "string"
         }],
         "Ulimits": [{
          "HardLimit": number,
          "Name": "string",
          "SoftLimit": number
         }],
         "User": "string",
         "VolumesFrom": [{
          "ReadOnly": boolean,
          "SourceContainer": "string"
         }],
         "WorkingDirectory": "string"
        }],
        "Cpu": "string",
        "ExecutionRoleArn": "string",
        "Family": "string",
        "InferenceAccelerators": [{
         "DeviceName": "string",
         "DeviceType": "string"
        }],
        "IpcMode": "string",
        "Memory": "string",
        "NetworkMode": "string",
        "PidMode": "string",
        "PlacementConstraints": [{
         "Expression": "string",
         "Type": "string"
        }],
        "ProxyConfiguration": {
```

```
        "ContainerName": "string",
        "ProxyConfigurationProperties": [{
         "Name": "string",
         "Value": "string"
        }],
        "Type": "string"
       },
       "RequiresCompatibilities": ["string"],
       "Status": "string",
       "TaskRoleArn": "string",
       "Volumes": [{
        "DockerVolumeConfiguration": {
         "Autoprovision": boolean,
         "Driver": "string",
         "DriverOpts": {
          "string": "string"
         },
         "Labels": {
          "string": "string"
         },
         "Scope": "string"
        },
        "EfsVolumeConfiguration": {
         "AuthorizationConfig": {
          "AccessPointId": "string",
          "Iam": "string"
         },
         "FilesystemId": "string",
         "RootDirectory": "string",
         "TransitEncryption": "string",
         "TransitEncryptionPort": number
        },
        "Host": {
         "SourcePath": "string"
        },
        "Name": "string"
       }]
      },
      "AwsEfsAccessPoint": {
       "AccessPointId": "string",
       "Arn": "string",
       "ClientToken": "string",
       "FileSystemId": "string",
       "PosixUser": {
```

```
        "Gid": "string",
        "SecondaryGids": ["string"],
        "Uid": "string"
       },
       "RootDirectory": {
        "CreationInfo": {
         "OwnerGid": "string",
         "OwnerUid": "string",
         "Permissions": "string"
        },
        "Path": "string"
       }
      },
      "AwsEksCluster": {
       "Arn": "string",
       "CertificateAuthorityData": "string",
       "ClusterStatus": "string",
       "Endpoint": "string",
       "Logging": {
        "ClusterLogging": [{
         "Enabled": boolean,
         "Types": ["string"]
        }]
       },
       "Name": "string",
       "ResourcesVpcConfig": {
        "EndpointPublicAccess": boolean,
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "RoleArn": "string",
       "Version": "string"
      },
      "AwsElasticBeanstalkEnvironment": {
       "ApplicationName": "string",
       "Cname": "string",
       "DateCreated": "string",
       "DateUpdated": "string",
       "Description": "string",
       "EndpointUrl": "string",
       "EnvironmentArn": "string",
       "EnvironmentId": "string",
       "EnvironmentLinks": [{
        "EnvironmentName": "string",
```

```
        "LinkName": "string"
       }],
       "EnvironmentName": "string",
       "OptionSettings": [{
        "Namespace": "string",
        "OptionName": "string",
        "ResourceName": "string",
        "Value": "string"
       }],
       "PlatformArn": "string",
       "SolutionStackName": "string",
       "Status": "string",
       "Tier": {
        "Name": "string",
        "Type": "string",
        "Version": "string"
       },
       "VersionLabel": "string"
      },
      "AwsElasticSearchDomain": {
       "AccessPolicies": "string",
       "DomainStatus": {
        "DomainId": "string",
        "DomainName": "string",
        "Endpoint": "string",
        "Endpoints": {
         "string": "string"
        }
       },
       "DomainEndpointOptions": {
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
       },
       "ElasticsearchClusterConfig": {
        "DedicatedMasterCount": number,
        "DedicatedMasterEnabled": boolean,
        "DedicatedMasterType": "string",
        "InstanceCount": number,
        "InstanceType": "string",
        "ZoneAwarenessConfig": {
         "AvailabilityZoneCount": number
        },
        "ZoneAwarenessEnabled": boolean
       },
```

```
        "ElasticsearchVersion": "string",
        "EncryptionAtRestOptions": {
         "Enabled": boolean,
         "KmsKeyId": "string"
        },
        "LogPublishingOptions": {
         "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         },
         "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
         }
        },
        "NodeToNodeEncryptionOptions": {
         "Enabled": boolean
        },
        "ServiceSoftwareOptions": {
         "AutomatedUpdateDate": "string",
         "Cancellable": boolean,
         "CurrentVersion": "string",
         "Description": "string",
         "NewVersion": "string",
         "UpdateAvailable": boolean,
         "UpdateStatus": "string"
        },
        "VPCOptions": {
         "AvailabilityZones": [
          "string"
         ],
         "SecurityGroupIds": [
          "string"
         ],
         "SubnetIds": [
          "string"
         ],
         "VPCId": "string"
        }
       },
```

```
      "AwsElbLoadBalancer": {
       "AvailabilityZones": ["string"],
       "BackendServerDescriptions": [{
        "InstancePort": number,
        "PolicyNames": ["string"]
       }],
       "CanonicalHostedZoneName": "string",
       "CanonicalHostedZoneNameID": "string",
       "CreatedTime": "string",
       "DnsName": "string",
       "HealthCheck": {
        "HealthyThreshold": number,
        "Interval": number,
        "Target": "string",
        "Timeout": number,
        "UnhealthyThreshold": number
       },
       "Instances": [{
        "InstanceId": "string"
       }],
       "ListenerDescriptions": [{
        "Listener": {
         "InstancePort": number,
         "InstanceProtocol": "string",
         "LoadBalancerPort": number,
         "Protocol": "string",
         "SslCertificateId": "string"
        },
        "PolicyNames": ["string"]
       }],
       "LoadBalancerAttributes": {
        "AccessLog": {
         "EmitInterval": number,
         "Enabled": boolean,
         "S3BucketName": "string",
         "S3BucketPrefix": "string"
        },
        "ConnectionDraining": {
         "Enabled": boolean,
         "Timeout": number
        },
        "ConnectionSettings": {
         "IdleTimeout": number
        },
```

```
        "CrossZoneLoadBalancing": {
         "Enabled": boolean
        },
        "AdditionalAttributes": [{
                        "Key": "string",
                        "Value": "string"
                    }]
       },
       "LoadBalancerName": "string",
       "Policies": {
        "AppCookieStickinessPolicies": [{
         "CookieName": "string",
         "PolicyName": "string"
        }],
        "LbCookieStickinessPolicies": [{
         "CookieExpirationPeriod": number,
         "PolicyName": "string"
        }],
        "OtherPolicies": ["string"]
       },
       "Scheme": "string",
       "SecurityGroups": ["string"],
       "SourceSecurityGroup": {
        "GroupName": "string",
        "OwnerAlias": "string"
       },
       "Subnets": ["string"],
       "VpcId": "string"
      },
      "AwsElbv2LoadBalancer": {
       "AvailabilityZones": {
        "SubnetId": "string",
        "ZoneName": "string"
       },
       "CanonicalHostedZoneId": "string",
       "CreatedTime": "string",
       "DNSName": "string",
       "IpAddressType": "string",
       "LoadBalancerAttributes": [{
        "Key": "string",
        "Value": "string"
       }],
       "Scheme": "string",
       "SecurityGroups": ["string"],
```

```
        "State": {
         "Code": "string",
         "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
       },
       "AwsEventSchemasRegistry": {
        "Description": "string",
        "RegistryArn": "string",
        "RegistryName": "string"
       },
       "AwsEventsEndpoint": {
        "Arn": "string",
        "Description": "string",
        "EndpointId": "string",
        "EndpointUrl": "string",
        "EventBuses": [
            {
                "EventBusArn": "string"
            },
            {
                "EventBusArn": "string"
            }
        ],
        "Name": "string",
        "ReplicationConfig": {
            "State": "string"
        },
        "RoleArn": "string",
        "RoutingConfig": {
            "FailoverConfig": {
                "Primary": {
                    "HealthCheck": "string"
                },
                "Secondary": {
                    "Route": "string"
                }
            }
        },
        "State": "string"
       },
       "AwsEventsEventBus": {
        "Arn": "string",
```

```
        "Name": "string",
        "Policy": "string"
      },
      "AwsGuardDutyDetector": {
        "FindingPublishingFrequency": "string",
        "ServiceRole": "string",
        "Status": "string",
        "DataSources": {
          "CloudTrail": {
            "Status": "string"
          },
          "DnsLogs": {
            "Status": "string"
          },
          "FlowLogs": {
            "Status": "string"
          },
          "S3Logs": {
            "Status": "string"
          },
          "Kubernetes": {
            "AuditLogs": {
              "Status": "string"
            }
          },
          "MalwareProtection": {
            "ScanEc2InstanceWithFindings": {
              "EbsVolumes": {
                "Status": "string"
              }
            },
            "ServiceRole": "string"
          }
        }
      },
      "AwsIamAccessKey": {
        "AccessKeyId": "string",
        "AccountId": "string",
        "CreatedAt": "string",
        "PrincipalId": "string",
        "PrincipalName": "string",
        "PrincipalType": "string",
        "SessionContext": {
          "Attributes": {
```

```
          "CreationDate": "string",
          "MfaAuthenticated": boolean
         },
         "SessionIssuer": {
          "AccountId": "string",
          "Arn": "string",
          "PrincipalId": "string",
          "Type": "string",
          "UserName": "string"
         }
        },
        "Status": "string"
       },
       "AwsIamGroup": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupId": "string",
        "GroupName": "string",
        "GroupPolicyList": [{
         "PolicyName": "string"
        }],
        "Path": "string"
       },
       "AwsIamPolicy": {
        "AttachmentCount": number,
        "CreateDate": "string",
        "DefaultVersionId": "string",
        "Description": "string",
        "IsAttachable": boolean,
        "Path": "string",
        "PermissionsBoundaryUsageCount": number,
        "PolicyId": "string",
        "PolicyName": "string",
        "PolicyVersionList": [{
         "CreateDate": "string",
         "IsDefaultVersion": boolean,
         "VersionId": "string"
        }],
        "UpdateDate": "string"
       },
       "AwsIamRole": {
```

```
        "AssumeRolePolicyDocument": "string",
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "InstanceProfileList": [{
         "Arn": "string",
         "CreateDate": "string",
         "InstanceProfileId": "string",
         "InstanceProfileName": "string",
         "Path": "string",
         "Roles": [{
          "Arn": "string",
          "AssumeRolePolicyDocument": "string",
          "CreateDate": "string",
          "Path": "string",
          "RoleId": "string",
          "RoleName": "string"
         }]
        }],
        "MaxSessionDuration": number,
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
        },
        "RoleId": "string",
        "RoleName": "string",
        "RolePolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsIamUser": {
        "AttachedManagedPolicies": [{
         "PolicyArn": "string",
         "PolicyName": "string"
        }],
        "CreateDate": "string",
        "GroupList": ["string"],
        "Path": "string",
        "PermissionsBoundary": {
         "PermissionsBoundaryArn": "string",
         "PermissionsBoundaryType": "string"
```

```
        },
        "UserId": "string",
        "UserName": "string",
        "UserPolicyList": [{
         "PolicyName": "string"
        }]
       },
       "AwsKinesisStream": {
        "Arn": "string",
        "Name": "string",
        "RetentionPeriodHours": number,
        "ShardCount": number,
        "StreamEncryption": {
         "EncryptionType": "string",
         "KeyId": "string"
        }
       },
       "AwsKmsKey": {
        "AWSAccountId": "string",
        "CreationDate": "string",
        "Description": "string",
        "KeyId": "string",
        "KeyManager": "string",
        "KeyRotationStatus": boolean,
        "KeyState": "string",
        "Origin": "string"
       },
       "AwsLambdaFunction": {
        "Architectures": [
         "string"
        ],
        "Code": {
         "S3Bucket": "string",
         "S3Key": "string",
         "S3ObjectVersion": "string",
         "ZipFile": "string"
        },
        "CodeSha256": "string",
        "DeadLetterConfig": {
         "TargetArn": "string"
        },
        "Environment": {
         "Variables": {
          "Stage": "string"
```

```
        },
        "Error": {
         "ErrorCode": "string",
         "Message": "string"
        }
       },
       "FunctionName": "string",
       "Handler": "string",
       "KmsKeyArn": "string",
       "LastModified": "string",
       "Layers": {
        "Arn": "string",
        "CodeSize": number
       },
       "PackageType": "string",
       "RevisionId": "string",
       "Role": "string",
       "Runtime": "string",
       "Timeout": integer,
       "TracingConfig": {
        "Mode": "string"
       },
       "Version": "string",
       "VpcConfig": {
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       },
       "MasterArn": "string",
       "MemorySize": number
      },
      "AwsLambdaLayerVersion": {
       "CompatibleRuntimes": [
        "string"
       ],
       "CreatedDate": "string",
       "Version": number
      },
      "AwsMskCluster": {
       "ClusterInfo": {
        "ClientAuthentication": {
         "Sasl": {
          "Scram": {
           "Enabled": boolean
          },
```

```
          "Iam": {
           "Enabled": boolean
          }
         },
         "Tls": {
          "CertificateAuthorityArnList": [],
          "Enabled": boolean
         },
         "Unauthenticated": {
          "Enabled": boolean
         }
        },
        "ClusterName": "string",
        "CurrentVersion": "string",
        "EncryptionInfo": {
         "EncryptionAtRest": {
          "DataVolumeKMSKeyId": "string"
         },
         "EncryptionInTransit": {
          "ClientBroker": "string",
          "InCluster": boolean
         }
        },
        "EnhancedMonitoring": "string",
        "NumberOfBrokerNodes": integer
       }
      },
      "AwsNetworkFirewallFirewall": {
       "DeleteProtection": boolean,
       "Description": "string",
       "FirewallArn": "string",
       "FirewallId": "string",
       "FirewallName": "string",
       "FirewallPolicyArn": "string",
       "FirewallPolicyChangeProtection": boolean,
       "SubnetChangeProtection": boolean,
       "SubnetMappings": [{
        "SubnetId": "string"
       }],
       "VpcId": "string"
      },
      "AwsNetworkFirewallFirewallPolicy": {
       "Description": "string",
       "FirewallPolicy": {
```

```
        "StatefulRuleGroupReferences": [{
         "ResourceArn": "string"
        }],
        "StatelessCustomActions": [{
         "ActionDefinition": {
          "PublishMetricAction": {
           "Dimensions": [{
            "Value": "string"
           }]
          }
         },
         "ActionName": "string"
        }],
        "StatelessDefaultActions": ["string"],
        "StatelessFragmentDefaultActions": ["string"],
        "StatelessRuleGroupReferences": [{
         "Priority": number,
         "ResourceArn": "string"
        }]
       },
       "FirewallPolicyArn": "string",
       "FirewallPolicyId": "string",
       "FirewallPolicyName": "string"
      },
      "AwsNetworkFirewallRuleGroup": {
       "Capacity": number,
       "Description": "string",
       "RuleGroup": {
        "RulesSource": {
         "RulesSourceList": {
          "GeneratedRulesType": "string",
          "Targets": ["string"],
          "TargetTypes": ["string"]
         },
         "RulesString": "string",
         "StatefulRules": [{
          "Action": "string",
          "Header": {
           "Destination": "string",
           "DestinationPort": "string",
           "Direction": "string",
           "Protocol": "string",
           "Source": "string",
           "SourcePort": "string"
```

```
          },
          "RuleOptions": [{
           "Keyword": "string",
           "Settings": ["string"]
          }]
         }],
         "StatelessRulesAndCustomActions": {
          "CustomActions": [{
           "ActionDefinition": {
            "PublishMetricAction": {
             "Dimensions": [{
              "Value": "string"
             }]
            }
           },
           "ActionName": "string"
          }],
          "StatelessRules": [{
           "Priority": number,
           "RuleDefinition": {
            "Actions": ["string"],
            "MatchAttributes": {
             "DestinationPorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Destinations": [{
              "AddressDefinition": "string"
             }],
             "Protocols": [number],
             "SourcePorts": [{
              "FromPort": number,
              "ToPort": number
             }],
             "Sources": [{
              "AddressDefinition": "string"
             }],
             "TcpFlags": [{
              "Flags": ["string"],
              "Masks": ["string"]
             }]
            }
           }
          }]
```

```
          }
         },
         "RuleVariables": {
          "IpSets": {
           "Definition": ["string"]
          },
          "PortSets": {
           "Definition": ["string"]
          }
         }
        },
        "RuleGroupArn": "string",
        "RuleGroupId": "string",
        "RuleGroupName": "string",
        "Type": "string"
       },
       "AwsOpenSearchServiceDomain": {
        "AccessPolicies": "string",
        "AdvancedSecurityOptions": {
         "Enabled": boolean,
         "InternalUserDatabaseEnabled": boolean,
         "MasterUserOptions": {
          "MasterUserArn": "string",
          "MasterUserName": "string",
          "MasterUserPassword": "string"
         }
        },
        "Arn": "string",
        "ClusterConfig": {
         "DedicatedMasterCount": number,
         "DedicatedMasterEnabled": boolean,
         "DedicatedMasterType": "string",
         "InstanceCount": number,
         "InstanceType": "string",
         "WarmCount": number,
         "WarmEnabled": boolean,
         "WarmType": "string",
         "ZoneAwarenessConfig": {
          "AvailabilityZoneCount": number
         },
         "ZoneAwarenessEnabled": boolean
        },
        "DomainEndpoint": "string",
        "DomainEndpointOptions": {
```

```
        "CustomEndpoint": "string",
        "CustomEndpointCertificateArn": "string",
        "CustomEndpointEnabled": boolean,
        "EnforceHTTPS": boolean,
        "TLSSecurityPolicy": "string"
      },
      "DomainEndpoints": {
        "string": "string"
      },
      "DomainName": "string",
      "EncryptionAtRestOptions": {
        "Enabled": boolean,
        "KmsKeyId": "string"
      },
      "EngineVersion": "string",
      "Id": "string",
      "LogPublishingOptions": {
        "AuditLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        },
        "IndexSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        },
        "SearchSlowLogs": {
          "CloudWatchLogsLogGroupArn": "string",
          "Enabled": boolean
        }
      },
      "NodeToNodeEncryptionOptions": {
        "Enabled": boolean
      },
      "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "string",
        "Cancellable": boolean,
        "CurrentVersion": "string",
        "Description": "string",
        "NewVersion": "string",
        "OptionalDeployment": boolean,
        "UpdateAvailable": boolean,
        "UpdateStatus": "string"
      },
      "VpcOptions": {
```

```
        "SecurityGroupIds": ["string"],
        "SubnetIds": ["string"]
       }
      },
      "AwsRdsDbCluster": {
       "ActivityStreamStatus": "string",
       "AllocatedStorage": number,
       "AssociatedRoles": [{
        "RoleArn": "string",
        "Status": "string"
       }],
       "AutoMinorVersionUpgrade": boolean,
       "AvailabilityZones": ["string"],
       "BackupRetentionPeriod": integer,
       "ClusterCreateTime": "string",
       "CopyTagsToSnapshot": boolean,
       "CrossAccountClone": boolean,
       "CustomEndpoints": ["string"],
       "DatabaseName": "string",
       "DbClusterIdentifier": "string",
       "DbClusterMembers": [{
        "DbClusterParameterGroupStatus": "string",
        "DbInstanceIdentifier": "string",
        "IsClusterWriter": boolean,
        "PromotionTier": integer
       }],
       "DbClusterOptionGroupMemberships": [{
        "DbClusterOptionGroupName": "string",
        "Status": "string"
       }],
       "DbClusterParameterGroup": "string",
       "DbClusterResourceId": "string",
       "DbSubnetGroup": "string",
       "DeletionProtection": boolean,
       "DomainMemberships": [{
        "Domain": "string",
        "Fqdn": "string",
        "IamRoleName": "string",
        "Status": "string"
       }],
       "EnabledCloudwatchLogsExports": ["string"],
       "Endpoint": "string",
       "Engine": "string",
       "EngineMode": "string",
```

```
        "EngineVersion": "string",
        "HostedZoneId": "string",
        "HttpEndpointEnabled": boolean,
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "MasterUsername": "string",
        "MultiAz": boolean,
        "Port": integer,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ReaderEndpoint": "string",
        "ReadReplicaIdentifiers": ["string"],
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRdsDbClusterSnapshot": {
        "AllocatedStorage": integer,
        "AvailabilityZones": ["string"],
        "ClusterCreateTime": "string",
        "DbClusterIdentifier": "string",
        "DbClusterSnapshotAttributes": [{
         "AttributeName": "string",
         "AttributeValues": ["string"]
        }],
        "DbClusterSnapshotIdentifier": "string",
        "Engine": "string",
        "EngineVersion": "string",
        "IamDatabaseAuthenticationEnabled": boolean,
        "KmsKeyId": "string",
        "LicenseModel": "string",
        "MasterUsername": "string",
        "PercentProgress": integer,
        "Port": integer,
        "SnapshotCreateTime": "string",
        "SnapshotType": "string",
        "Status": "string",
        "StorageEncrypted": boolean,
        "VpcId": "string"
       },
       "AwsRdsDbInstance": {
```

```
        "AllocatedStorage": number,
        "AssociatedRoles": [{
         "RoleArn": "string",
         "FeatureName": "string",
         "Status": "string"
        }],
        "AutoMinorVersionUpgrade": boolean,
        "AvailabilityZone": "string",
        "BackupRetentionPeriod": number,
        "CACertificateIdentifier": "string",
        "CharacterSetName": "string",
        "CopyTagsToSnapshot": boolean,
        "DBClusterIdentifier": "string",
        "DBInstanceClass": "string",
        "DBInstanceIdentifier": "string",
        "DbInstancePort": number,
        "DbInstanceStatus": "string",
        "DbiResourceId": "string",
        "DBName": "string",
        "DbParameterGroups": [{
         "DbParameterGroupName": "string",
         "ParameterApplyStatus": "string"
        }],
        "DbSecurityGroups": ["string"],
        "DbSubnetGroup": {
         "DbSubnetGroupArn": "string",
         "DbSubnetGroupDescription": "string",
         "DbSubnetGroupName": "string",
         "SubnetGroupStatus": "string",
         "Subnets": [{
          "SubnetAvailabilityZone": {
           "Name": "string"
          },
          "SubnetIdentifier": "string",
          "SubnetStatus": "string"
         }],
         "VpcId": "string"
        },
        "DeletionProtection": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number,
         "HostedZoneId": "string"
        },
```

```
        "DomainMemberships": [{
         "Domain": "string",
         "Fqdn": "string",
         "IamRoleName": "string",
         "Status": "string"
        }],
        "EnabledCloudwatchLogsExports": ["string"],
        "Engine": "string",
        "EngineVersion": "string",
        "EnhancedMonitoringResourceArn": "string",
        "IAMDatabaseAuthenticationEnabled": boolean,
        "InstanceCreateTime": "string",
        "Iops": number,
        "KmsKeyId": "string",
        "LatestRestorableTime": "string",
        "LicenseModel": "string",
        "ListenerEndpoint": {
         "Address": "string",
         "HostedZoneId": "string",
         "Port": number
        },
        "MasterUsername": "admin",
        "MaxAllocatedStorage": number,
        "MonitoringInterval": number,
        "MonitoringRoleArn": "string",
        "MultiAz": boolean,
        "OptionGroupMemberships": [{
         "OptionGroupName": "string",
         "Status": "string"
        }],
        "PendingModifiedValues": {
         "AllocatedStorage": number,
         "BackupRetentionPeriod": number,
         "CaCertificateIdentifier": "string",
         "DbInstanceClass": "string",
         "DbInstanceIdentifier": "string",
         "DbSubnetGroupName": "string",
         "EngineVersion": "string",
         "Iops": number,
         "LicenseModel": "string",
         "MasterUserPassword": "string",
         "MultiAZ": boolean,
         "PendingCloudWatchLogsExports": {
          "LogTypesToDisable": ["string"],
```

```
          "LogTypesToEnable": ["string"]
         },
         "Port": number,
         "ProcessorFeatures": [{
          "Name": "string",
          "Value": "string"
         }],
         "StorageType": "string"
        },
        "PerformanceInsightsEnabled": boolean,
        "PerformanceInsightsKmsKeyId": "string",
        "PerformanceInsightsRetentionPeriod": number,
        "PreferredBackupWindow": "string",
        "PreferredMaintenanceWindow": "string",
        "ProcessorFeatures": [{
         "Name": "string",
         "Value": "string"
        }],
        "PromotionTier": number,
        "PubliclyAccessible": boolean,
        "ReadReplicaDBClusterIdentifiers": ["string"],
        "ReadReplicaDBInstanceIdentifiers": ["string"],
        "ReadReplicaSourceDBInstanceIdentifier": "string",
        "SecondaryAvailabilityZone": "string",
        "StatusInfos": [{
         "Message": "string",
         "Normal": boolean,
         "Status": "string",
         "StatusType": "string"
        }],
        "StorageEncrypted": boolean,
        "TdeCredentialArn": "string",
        "Timezone": "string",
        "VpcSecurityGroups": [{
         "VpcSecurityGroupId": "string",
         "Status": "string"
        }]
       },
       "AwsRdsDbSecurityGroup": {
        "DbSecurityGroupArn": "string",
        "DbSecurityGroupDescription": "string",
        "DbSecurityGroupName": "string",
        "Ec2SecurityGroups": [{
         "Ec2SecurityGroupuId": "string",
```

```
        "Ec2SecurityGroupName": "string",
        "Ec2SecurityGroupOwnerId": "string",
        "Status": "string"
       }],
       "IpRanges": [{
        "CidrIp": "string",
        "Status": "string"
       }],
       "OwnerId": "string",
       "VpcId": "string"
      },
      "AwsRdsDbSnapshot": {
       "AllocatedStorage": integer,
       "AvailabilityZone": "string",
       "DbInstanceIdentifier": "string",
       "DbiResourceId": "string",
       "DbSnapshotIdentifier": "string",
       "Encrypted": boolean,
       "Engine": "string",
       "EngineVersion": "string",
       "IamDatabaseAuthenticationEnabled": boolean,
       "InstanceCreateTime": "string",
       "Iops": number,
       "KmsKeyId": "string",
       "LicenseModel": "string",
       "MasterUsername": "string",
       "OptionGroupName": "string",
       "PercentProgress": integer,
       "Port": integer,
       "ProcessorFeatures": [],
       "SnapshotCreateTime": "string",
       "SnapshotType": "string",
       "SourceDbSnapshotIdentifier": "string",
       "SourceRegion": "string",
       "Status": "string",
       "StorageType": "string",
       "TdeCredentialArn": "string",
       "Timezone": "string",
       "VpcId": "string"
      },
      "AwsRdsEventSubscription": {
       "CustomerAwsId": "string",
       "CustSubscriptionId": "string",
       "Enabled": boolean,
```

```
        "EventCategoriesList": ["string"],
        "EventSubscriptionArn": "string",
        "SnsTopicArn": "string",
        "SourceIdsList": ["string"],
        "SourceType": "string",
        "Status": "string",
        "SubscriptionCreationTime": "string"
       },
       "AwsRedshiftCluster": {
        "AllowVersionUpgrade": boolean,
        "AutomatedSnapshotRetentionPeriod": number,
        "AvailabilityZone": "string",
        "ClusterAvailabilityStatus": "string",
        "ClusterCreateTime": "string",
        "ClusterIdentifier": "string",
        "ClusterNodes": [{
         "NodeRole": "string",
         "PrivateIPAddress": "string",
         "PublicIPAddress": "string"
        }],
        "ClusterParameterGroups": [{
         "ClusterParameterStatusList": [{
          "ParameterApplyErrorDescription": "string",
          "ParameterApplyStatus": "string",
          "ParameterName": "string"
         }],
         "ParameterApplyStatus": "string",
         "ParameterGroupName": "string"
        }],
        "ClusterPublicKey": "string",
        "ClusterRevisionNumber": "string",
        "ClusterSecurityGroups": [{
         "ClusterSecurityGroupName": "string",
         "Status": "string"
        }],
        "ClusterSnapshotCopyStatus": {
         "DestinationRegion": "string",
         "ManualSnapshotRetentionPeriod": number,
         "RetentionPeriod": number,
         "SnapshotCopyGrantName": "string"
        },
        "ClusterStatus": "string",
        "ClusterSubnetGroupName": "string",
        "ClusterVersion": "string",
```

```
        "DBName": "string",
        "DeferredMaintenanceWindows": [{
         "DeferMaintenanceEndTime": "string",
         "DeferMaintenanceIdentifier": "string",
         "DeferMaintenanceStartTime": "string"
        }],
        "ElasticIpStatus": {
         "ElasticIp": "string",
         "Status": "string"
        },
        "ElasticResizeNumberOfNodeOptions": "string",
        "Encrypted": boolean,
        "Endpoint": {
         "Address": "string",
         "Port": number
        },
        "EnhancedVpcRouting": boolean,
        "ExpectedNextSnapshotScheduleTime": "string",
        "ExpectedNextSnapshotScheduleTimeStatus": "string",
        "HsmStatus": {
         "HsmClientCertificateIdentifier": "string",
         "HsmConfigurationIdentifier": "string",
         "Status": "string"
        },
        "IamRoles": [{
         "ApplyStatus": "string",
         "IamRoleArn": "string"
        }],
        "KmsKeyId": "string",
        "LoggingStatus":{
                    "BucketName": "string",
                    "LastFailureMessage": "string",
                    "LastFailureTime": "string",
                    "LastSuccessfulDeliveryTime": "string",
                    "LoggingEnabled": boolean,
                    "S3KeyPrefix": "string"
                },
        "MaintenanceTrackName": "string",
        "ManualSnapshotRetentionPeriod": number,
        "MasterUsername": "string",
        "NextMaintenanceWindowStartTime": "string",
        "NodeType": "string",
        "NumberOfNodes": number,
        "PendingActions": ["string"],
```

```
        "PendingModifiedValues": {
         "AutomatedSnapshotRetentionPeriod": number,
         "ClusterIdentifier": "string",
         "ClusterType": "string",
         "ClusterVersion": "string",
         "EncryptionType": "string",
         "EnhancedVpcRouting": boolean,
         "MaintenanceTrackName": "string",
         "MasterUserPassword": "string",
         "NodeType": "string",
         "NumberOfNodes": number,
         "PubliclyAccessible": "string"
        },
        "PreferredMaintenanceWindow": "string",
        "PubliclyAccessible": boolean,
        "ResizeInfo": {
         "AllowCancelResize": boolean,
         "ResizeType": "string"
        },
        "RestoreStatus": {
         "CurrentRestoreRateInMegaBytesPerSecond": number,
         "ElapsedTimeInSeconds": number,
         "EstimatedTimeToCompletionInSeconds": number,
         "ProgressInMegaBytes": number,
         "SnapshotSizeInMegaBytes": number,
         "Status": "string"
        },
        "SnapshotScheduleIdentifier": "string",
        "SnapshotScheduleState": "string",
        "VpcId": "string",
        "VpcSecurityGroups": [{
         "Status": "string",
         "VpcSecurityGroupId": "string"
        }]
       },
       "AwsRoute53HostedZone": {
        "HostedZone": {
         "Id": "string",
         "Name": "string",
         "Config": {
          "Comment": "string"
         }
        },
        "NameServers": ["string"],
```

```
        "QueryLoggingConfig": {
         "CloudWatchLogsLogGroupArn": {
          "CloudWatchLogsLogGroupArn": "string",
          "Id": "string",
          "HostedZoneId": "string"
         }
        },
        "Vpcs": [
         {
          "Id": "string",
          "Region": "string"
         }
        ]
       },
       "AwsS3AccessPoint": {
        "AccessPointArn": "string",
        "Alias": "string",
        "Bucket": "string",
        "BucketAccountId": "string",
        "Name": "string",
        "NetworkOrigin": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "VpcConfiguration": {
         "VpcId": "string"
        }
       },
       "AwsS3AccountPublicAccessBlock": {
        "BlockPublicAcls": boolean,
        "BlockPublicPolicy": boolean,
        "IgnorePublicAcls": boolean,
        "RestrictPublicBuckets": boolean
       },
       "AwsS3Bucket": {
        "AccessControlList": "string",
        "BucketLifecycleConfiguration": {
         "Rules": [{
          "AbortIncompleteMultipartUpload": {
           "DaysAfterInitiation": number
          },
```

```
          "ExpirationDate": "string",
          "ExpirationInDays": number,
          "ExpiredObjectDeleteMarker": boolean,
          "Filter": {
           "Predicate": {
            "Operands": [{
              "Prefix": "string",
              "Type": "string"
             },
             {
              "Tag": {
               "Key": "string",
               "Value": "string"
              },
              "Type": "string"
             }
            ],
            "Type": "string"
           }
          },
          "Id": "string",
          "NoncurrentVersionExpirationInDays": number,
          "NoncurrentVersionTransitions": [{
           "Days": number,
           "StorageClass": "string"
          }],
          "Prefix": "string",
          "Status": "string",
          "Transitions": [{
           "Date": "string",
           "Days": number,
           "StorageClass": "string"
          }]
         }]
        },
        "BucketLoggingConfiguration": {
         "DestinationBucketName": "string",
         "LogFilePrefix": "string"
        },
        "BucketName": "string",
        "BucketNotificationConfiguration": {
         "Configurations": [{
          "Destination": "string",
          "Events": ["string"],
```

```
          "Filter": {
           "S3KeyFilter": {
            "FilterRules": [{
             "Name": "string",
             "Value": "string"
            }]
           }
          },
          "Type": "string"
         }]
        },
        "BucketVersioningConfiguration": {
         "IsMfaDeleteEnabled": boolean,
         "Status": "string"
        },
        "BucketWebsiteConfiguration": {
         "ErrorDocument": "string",
         "IndexDocumentSuffix": "string",
         "RedirectAllRequestsTo": {
          "HostName": "string",
          "Protocol": "string"
         },
         "RoutingRules": [{
          "Condition": {
           "HttpErrorCodeReturnedEquals": "string",
           "KeyPrefixEquals": "string"
          },
          "Redirect": {
           "HostName": "string",
           "HttpRedirectCode": "string",
           "Protocol": "string",
           "ReplaceKeyPrefixWith": "string",
           "ReplaceKeyWith": "string"
          }
         }]
        },
        "CreatedAt": "string",
        "ObjectLockConfiguration": {
         "ObjectLockEnabled": "string",
         "Rule": {
          "DefaultRetention": {
           "Days": integer,
           "Mode": "string",
           "Years": integer
```

```
          }
         }
        },
        "OwnerAccountId": "string",
        "OwnerId": "string",
        "OwnerName": "string",
        "PublicAccessBlockConfiguration": {
         "BlockPublicAcls": boolean,
         "BlockPublicPolicy": boolean,
         "IgnorePublicAcls": boolean,
         "RestrictPublicBuckets": boolean
        },
        "ServerSideEncryptionConfiguration": {
         "Rules": [{
          "ApplyServerSideEncryptionByDefault": {
           "KMSMasterKeyID": "string",
           "SSEAlgorithm": "string"
          }
         }]
        }
       },
       "AwsS3Object": {
        "ContentType": "string",
        "ETag": "string",
        "LastModified": "string",
        "ServerSideEncryption": "string",
        "SSEKMSKeyId": "string",
        "VersionId": "string"
       },
       "AwsSagemakerNotebookInstance": {
        "DirectInternetAccess": "string",
        "InstanceMetadataServiceConfiguration": {
         "MinimumInstanceMetadataServiceVersion": "string"
        },
        "InstanceType": "string",
        "LastModifiedTime": "string",
        "NetworkInterfaceId": "string",
        "NotebookInstanceArn": "string",
        "NotebookInstanceName": "string",
        "NotebookInstanceStatus": "string",
        "PlatformIdentifier": "string",
        "RoleArn": "string",
        "RootAccess": "string",
        "SecurityGroups": ["string"],
```

```
        "SubnetId": "string",
        "Url": "string",
        "VolumeSizeInGB": number
      },
      "AwsSecretsManagerSecret": {
        "Deleted": boolean,
        "Description": "string",
        "KmsKeyId": "string",
        "Name": "string",
        "RotationEnabled": boolean,
        "RotationLambdaArn": "string",
        "RotationOccurredWithinFrequency": boolean,
        "RotationRules": {
          "AutomaticallyAfterDays": integer
        }
      },
      "AwsSnsTopic": {
        "ApplicationSuccessFeedbackRoleArn": "string",
        "FirehoseFailureFeedbackRoleArn": "string",
        "FirehoseSuccessFeedbackRoleArn": "string",
        "HttpFailureFeedbackRoleArn": "string",
        "HttpSuccessFeedbackRoleArn": "string",
        "KmsMasterKeyId": "string",
        "Owner": "string",
        "SqsFailureFeedbackRoleArn": "string",
        "SqsSuccessFeedbackRoleArn": "string",
        "Subscription": {
          "Endpoint": "string",
          "Protocol": "string"
        },
        "TopicName": "string"
      },
      "AwsSqsQueue": {
        "DeadLetterTargetArn": "string",
        "KmsDataKeyReusePeriodSeconds": number,
        "KmsMasterKeyId": "string",
        "QueueName": "string"
      },
      "AwsSsmPatchCompliance": {
        "Patch": {
          "ComplianceSummary": {
            "ComplianceType": "string",
            "CompliantCriticalCount": integer,
            "CompliantHighCount": integer,
```

```
          "CompliantInformationalCount": integer,
          "CompliantLowCount": integer,
          "CompliantMediumCount": integer,
          "CompliantUnspecifiedCount": integer,
          "ExecutionType": "string",
          "NonCompliantCriticalCount": integer,
          "NonCompliantHighCount": integer,
          "NonCompliantInformationalCount": integer,
          "NonCompliantLowCount": integer,
          "NonCompliantMediumCount": integer,
          "NonCompliantUnspecifiedCount": integer,
          "OverallSeverity": "string",
          "PatchBaselineId": "string",
          "PatchGroup": "string",
          "Status": "string"
        }
       }
      },
      "AwsStepFunctionStateMachine": {
       "StateMachineArn": "string",
       "Name": "string",
       "Status": "string",
       "RoleArn": "string",
       "Type": "string",
       "LoggingConfiguration": {
        "Level": "string",
        "IncludeExecutionData": boolean
       },
       "TracingConfiguration": {
        "Enabled": boolean
       }
      },
      "AwsWafRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
```

```
      "AwsWafRegionalRateBasedRule": {
       "MatchPredicates": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "MetricName": "string",
       "Name": "string",
       "RateKey": "string",
       "RateLimit": number,
       "RuleId": "string"
      },
      "AwsWafRegionalRule": {
       "MetricName": "string",
       "Name": "string",
       "RuleId": "string",
       "PredicateList": [{
           "DataId": "string",
           "Negated": boolean,
           "Type": "string"
       }]
      },
      "AwsWafRegionalRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafRegionalWebAcl": {
       "DefaultAction": "string",
       "MetricName" : "string",
       "Name": "string",
       "RulesList" : [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
```

```
        "RuleId": "string",
        "Type": "string",
        "ExcludedRules": [{
         "ExclusionType": "string",
         "RuleId": "string"
        }],
        "OverrideAction": {
         "Type": "string"
        }
       }],
       "WebAclId": "string"
      },
      "AwsWafRule": {
       "MetricName": "string",
       "Name": "string",
       "PredicateList": [{
        "DataId": "string",
        "Negated": boolean,
        "Type": "string"
       }],
       "RuleId": "string"
      },
      "AwsWafRuleGroup": {
       "MetricName": "string",
       "Name": "string",
       "RuleGroupId": "string",
       "Rules": [{
        "Action": {
         "Type": "string"
        },
        "Priority": number,
        "RuleId": "string",
        "Type": "string"
       }]
      },
      "AwsWafv2RuleGroup": {
       "Arn": "string",
       "Capacity": number,
       "Description": "string",
       "Id": "string",
       "Name": "string",
       "Rules": [{
        "Action": {
        "Allow": {
```

```
          "CustomRequestHandling": {
           "InsertHeaders": [
            {
            "Name": "string",
            "Value": "string"
            },
            {
            "Name": "string",
            "Value": "string"
            }
           ]
          }
         }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string",
          "SampledRequestsEnabled": boolean
         }
        }],
        "VisibilityConfig": {
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string",
         "SampledRequestsEnabled": boolean
        }
       },
       "AwsWafWebAcl": {
        "DefaultAction": "string",
        "Name": "string",
        "Rules": [{
         "Action": {
          "Type": "string"
         },
         "ExcludedRules": [{
          "RuleId": "string"
         }],
         "OverrideAction": {
          "Type": "string"
         },
         "Priority": number,
         "RuleId": "string",
         "Type": "string"
```

```
        }],
        "WebAclId": "string"
       },
       "AwsWafv2WebAcl": {
        "Arn": "string",
        "Capacity": number,
        "CaptchaConfig": {
         "ImmunityTimeProperty": {
          "ImmunityTime": number
         }
        },
        "DefaultAction": {
         "Block": {}
        },
        "Description": "string",
        "ManagedbyFirewallManager": boolean,
        "Name": "string",
        "Rules": [{
         "Action": {
          "RuleAction": {
           "Block": {}
          }
         },
         "Name": "string",
         "Priority": number,
         "VisibilityConfig": {
          "SampledRequestsEnabled": boolean,
          "CloudWatchMetricsEnabled": boolean,
          "MetricName": "string"
         }
        }],
        "VisibilityConfig": {
         "SampledRequestsEnabled": boolean,
         "CloudWatchMetricsEnabled": boolean,
         "MetricName": "string"
        }
       },
       "AwsXrayEncryptionConfig": {
        "KeyId": "string",
        "Status": "string",
        "Type": "string"
       },
       "CodeRepository": {
        "CodeSecurityIntegrationArn": "string",
```

```
        "ProjectName": "string",
        "ProviderType": "string"
       },
       "Container": {
        "ContainerRuntime": "string",
        "ImageId": "string",
        "ImageName": "string",
        "LaunchedAt": "string",
        "Name": "string",
        "Privileged": boolean,
        "VolumeMounts": [{
         "Name": "string",
         "MountPath": "string"
        }]
       },
       "Other": {
        "string": "string"
       },
       "Id": "string",
       "Partition": "string",
       "Region": "string",
       "ResourceRole": "string",
       "Tags": {
        "string": "string"
       },
       "Type": "string"
      }],
      "SchemaVersion": "string",
      "Severity": {
       "Label": "string",
       "Normalized": number,
       "Original": "string"
      },
      "Sample": boolean,
      "SourceUrl": "string",
      "Threats": [{
       "FilePaths": [{
        "FileName": "string",
        "FilePath": "string",
        "Hash": "string",
        "ResourceId": "string"
       }],
       "ItemCount": number,
       "Name": "string",
```

```
      "Severity": "string"
     }],
     "ThreatIntelIndicators": [{
      "Category": "string",
      "LastObservedAt": "string",
      "Source": "string",
      "SourceUrl": "string",
      "Type": "string",
      "Value": "string"
     }],
     "Title": "string",
     "Types": ["string"],
     "UpdatedAt": "string",
     "UserDefinedFields": {
      "string": "string"
     },
     "VerificationState": "string",
     "Vulnerabilities": [{
      "CodeVulnerabilities": [{
       "Cwes": [
        "string",
        "string"
       ],
       "FilePath": {
        "EndLine": integer,
        "FileName": "string",
        "FilePath": "string",
        "StartLine": integer
       },
       "SourceArn":"string"
      }],
      "Cvss": [{
       "Adjustments": [{
        "Metric": "string",
        "Reason": "string"
       }],
       "BaseScore": number,
       "BaseVector": "string",
       "Source": "string",
       "Version": "string"
      }],
      "EpssScore": number,
      "ExploitAvailable": "string",
      "FixAvailable": "string",
```

```
      "Id": "string",
      "LastKnownExploitAt": "string",
      "ReferenceUrls": ["string"],
      "RelatedVulnerabilities": ["string"],
      "Vendor": {
       "Name": "string",
       "Url": "string",
       "VendorCreatedAt": "string",
       "VendorSeverity": "string",
       "VendorUpdatedAt": "string"
      },
      "VulnerablePackages": [{
       "Architecture": "string",
       "Epoch": "string",
       "FilePath": "string",
       "FixedInVersion": "string",
       "Name": "string",
       "PackageManager": "string",
       "Release": "string",
       "Remediation": "string",
       "SourceLayerArn": "string",
       "SourceLayerHash": "string",
       "Version": "string"
      }]
     }],
     "Workflow": {
      "Status": "string"
     },
     "WorkflowState": "string"
    }
]
```

Dampak konsolidasi pada bidang dan nilai ASFF

AWS Security Hub CSPM menawarkan dua jenis konsolidasi untuk kontrol:

- Tampilan kontrol konsolidasi — Dengan jenis konsolidasi ini, setiap kontrol memiliki pengidentifikasi tunggal di semua standar. Selain itu, pada konsol CSPM Security Hub, halaman Kontrol menampilkan semua kontrol di semua standar.
- Temuan kontrol terkonsolidasi — Dengan jenis konsolidasi ini, Security Hub CSPM menghasilkan satu temuan untuk kontrol, bahkan jika kontrol tersebut berlaku untuk beberapa standar yang diaktifkan. Ini dapat mengurangi kebisingan pencarian.

Anda tidak dapat mengaktifkan atau menonaktifkan tampilan kontrol gabungan. Temuan kontrol konsolidasi diaktifkan secara default jika Anda mengaktifkan Security Hub CSPM pada atau setelah 23 Februari 2023. Jika tidak, itu dinonaktifkan secara default. Namun, untuk organisasi, temuan kontrol konsolidasi diaktifkan untuk akun anggota CSPM Security Hub hanya jika diaktifkan untuk akun administrator. Untuk mempelajari lebih lanjut tentang temuan kontrol konsolidasi, lihatMenghasilkan dan memperbarui temuan kontrol.

Kedua jenis konsolidasi mempengaruhi bidang dan nilai untuk temuan kontrol diAWS Format Penemuan Keamanan (ASFF).

Topik

- Tampilan kontrol konsolidasi - Perubahan ASFF
- Temuan kontrol konsolidasi — Perubahan ASFF
- ID Generator sebelum dan sesudah mengaktifkan temuan kontrol konsolidasi
- Bagaimana konsolidasi memengaruhi ID kontrol dan judul
- Memperbarui alur kerja untuk konsolidasi

Tampilan kontrol konsolidasi - Perubahan ASFF

Fitur tampilan kontrol konsolidasi memperkenalkan perubahan berikut pada bidang dan nilai untuk temuan kontrol di ASFF. Jika alur kerja Anda tidak bergantung pada nilai untuk bidang ASFF ini, tidak ada tindakan yang diperlukan. Jika Anda memiliki alur kerja yang bergantung pada nilai tertentu untuk bidang ini, perbarui alur kerja Anda untuk menggunakan nilai saat ini.

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol konsolidasi, dan deskripsi perubahan
Compliance.SecurityControlId	Tidak berlaku (bidang baru)	EC2.2 Memperkenalkan ID kontrol tunggal di seluruh standar. `ProductFields.RuleId` masih menyediakan ID kontrol berbasis standar untuk kontrol CIS v1.2.0. `ProductFields.Cont`

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol konsolidasi, dan deskripsi perubahan
		`rolId` masih menyediakan ID kontrol berbasis standar untuk kontrol dalam standar lain.
Compliance.AssociatedStandards	Tidak berlaku (bidang baru)	[{" StandardsId ":" standards /aws -dasar-keamanan-terbaik- /1.0.0 "}] practices/v Menunjukkan standar mana kontrol diaktifkan.
ProductFields.ArchivalReasons:0/Description	Tidak berlaku (bidang baru)	"Temuan ini dalam keadaan ARCHIVED karena temuan kontrol konsolidasi telah dihidupkan atau dimatikan. Hal ini menyebabkan temuan dalam keadaan sebelumnya diarsipkan ketika temuan baru dihasilkan." Menjelaskan mengapa Security Hub CSPM telah mengarsipkan temuan yang ada.
ProductFields.ArchivalReasons:0/ReasonCode	Tidak berlaku (bidang baru)	"PEMBARUAN_TEMUAN_KONTROL TERKONSOLIDASI" Memberikan alasan mengapa Security Hub CSPM telah mengarsipkan temuan yang ada.

Bidang ASFF	Nilai sampel sebelum tampilan kontrol konsolidasi	Nilai sampel setelah tampilan kontrol konsolidasi, dan deskripsi perubahan
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Bidang ini tidak lagi mereferensikan standar.
Remediation.Recommendation.Text	“Untuk petunjuk tentang cara memperbaiki masalah ini, lihat dokumentasi AWS Security Hub CSPM PCI DSS.”	“Untuk petunjuk tentang cara memperbaiki masalah ini, lihat dokumentasi kontrol CSPM Hub AWS Keamanan.” Bidang ini tidak lagi mereferensikan standar.
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Bidang ini tidak lagi mereferensikan standar.

Temuan kontrol konsolidasi — Perubahan ASFF

Jika Anda mengaktifkan temuan kontrol konsolidasi, Anda mungkin terpengaruh oleh perubahan berikut pada bidang dan nilai untuk temuan kontrol di ASFF. Perubahan ini merupakan tambahan dari perubahan yang diperkenalkan oleh fitur tampilan kontrol konsolidasi. Jika alur kerja Anda tidak bergantung pada nilai untuk bidang ASFF ini, tidak ada tindakan yang diperlukan. Jika Anda memiliki alur kerja yang bergantung pada nilai tertentu untuk bidang ini, perbarui alur kerja Anda untuk menggunakan nilai saat ini.

> **Tip**
>
> Jika Anda menggunakan solusi Respon Keamanan Otomatis pada AWS v2.0.0, perhatikan bahwa solusi ini mendukung temuan kontrol konsolidasi. Ini berarti Anda dapat mempertahankan alur kerja saat ini jika Anda mengaktifkan temuan kontrol konsolidasi.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
GeneratorId	aws-dasar-keamanan- terbaik- /1.0. practices/v 0/Config. 1	keamanan- control/Config .1 Bidang ini tidak lagi mereferen sikan standar.
judul	PCI.Config.1 AWS Config harus diaktifkan	AWS Config harus diaktifkan Bidang ini tidak lagi merujuk informasi khusus standar.
Id	arn: aws:hub keamanan: eu- central- 1:123456789012: - /3.2. subscription/pci dss/v 1/PCI. IAM.5/finding/ab6d6a26-a156 -48f0-9403-115983e5a956	arn: aws:hub keamanan: eu- central- 1:123456789012: keamanan-. control/iam 9/finding /ab6d6a26-a156-48f0-9403-11 5983e5a956 Bidang ini tidak lagi mereferen sikan standar.
ProductFields.ControlId	PCI.EC2.2	Dihapus. Lihat sebagai `Compliance.Securit yControlId` gantinya. Bidang ini dihapus demi ID kontrol agnostik standar tunggal.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
ProductFields.RuleId	1.3	Dihapus. Lihat sebagai `Compliance.Securit yControlId` gantinya. Bidang ini dihapus demi ID kontrol agnostik standar tunggal.
Deskripsi	Kontrol PCI DSS ini memeriksa apakah AWS Config diaktifkan di akun saat ini dan wilayah.	AWS Kontrol ini memeriksa apakah AWS Config diaktifkan di akun dan wilayah saat ini. Bidang ini tidak lagi mereferen sikan standar.

Kepelikan	“Tingkat keparahan”: {
	
	“Produk”: 90,
	
	“Label”: “KRITIS”,
	
	“Dinormalisasi”: 90,
	
	“Asli”: “KRITIS”
	
	}
		“Tingkat keparahan”: {
		
		“Label”: “KRITIS”,
		
		“Dinormalisasi”: 90,
		
		“Asli”: “KRITIS”
		
		}
		
		Security Hub CSPM tidak lagi menggunakan bidang Produk untuk menggambarkan tingkat keparahan temuan.

Tipe	["Perangkat Lunak dan Konfigura si Checks/Industry dan Per Standards/PCI-DSS aturan “]	["Perangkat Lunak dan Konfigura si Checks/Industry dan Standar Peraturan"] Bidang ini tidak lagi mereferen sikan standar.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
Compliance.Related Requirements	["PCI DSS 10.5.2", “PCI DSS 11.5", “Yayasan AWS CIS 2.5"]	["PCI DSS v3.2. 1/10.5.2", “PCI DSS v3.2. 1/110,5 “, “Benchmark AWS Yayasan CIS v1.2. 0/2.5"] Bidang ini menunjukkan persyarat an terkait di semua standar yang diaktifkan.
CreatedAt	2022-05-05 T08:18:13.138Z	2022-09-25 T08:18:13.138Z Format tetap sama, tetapi nilai disetel ulang saat Anda mengaktif kan temuan kontrol konsolidasi.
FirstObservedAt	2022-05-07 T08:18:13.138Z	2022-09-28 T08:18:13.138Z Format tetap sama, tetapi nilai disetel ulang saat Anda mengaktif kan temuan kontrol konsolidasi.
ProductFields.Reco mmendationUrl	https://docs.aws.amazon.com /console/securityhub/EC2.2/ remediation	Dihapus. Lihat sebagai `Remediation.Recomm endation.Url` gantinya.
ProductFields.Stan dardsArn	arn:aws:securityhub::: -dasar-ke amanan-terbaik- /1.0.0 standards/ aws practices/v	Dihapus. Lihat sebagai `Compliance.Associa tedStandards` gantinya.
ProductFields.Stan dardsControlArn	arn:aws:securityhub: us-east- 1:123456789012: -fundamental- security-best- /1.0. control/aws practices/v 0/Config.1	Dihapus. Security Hub CSPM menghasilkan satu temuan untuk pemeriksaan keamanan lintas standar.

Bidang ASFF	Nilai contoh sebelum mengaktif kan temuan kontrol konsolidasi	Contoh nilai setelah mengaktifkan temuan kontrol konsolidasi, dan deskripsi perubahan
ProductFields.Stan dardsGuideArn	arn:aws:securityhub::: -aws-fond asi- /1.2.0 ruleset/cis benchmark/ v	Dihapus. Lihat sebagai `Compliance.Associa tedStandards` gantinya.
ProductFields.Stan dardsGuideSubscrip tionArn	arn: aws:securityhub: us-east- 2:123456789012: -aws-foun dation- /1.2.0 subscription/cis benchmark/v	Dihapus. Security Hub CSPM menghasilkan satu temuan untuk pemeriksaan keamanan lintas standar.
ProductFields.Stan dardsSubscriptionArn	arn:aws:securityhub: us-east- 1:123456789012: -fundamental- security-best- /1.0.0 subscription/ aws practices/v	Dihapus. Security Hub CSPM menghasilkan satu temuan untuk pemeriksaan keamanan lintas standar.
ProductFields.aws/ securityhub/FindingId	arn:aws:securityhub: us-east-1 :: /:aws:securityhub: us-timur- 1:123456789012: -dasar-ke amanan-terbaik- /1.0. product/ aws securityhub/arn subscript ion/aws practices/v 0/Config. 1/finding/751c2173-7372-4e1 2-8656-a5210dfb1d67	arn:aws:securityhub: us-east-1 :: /:aws:securityhub: us-east- 1:123456789012: keamanan- . product/aws securityhub/arn control/Config 1/finding/751c2173 -7372-4e12-8656-a5210dfb1d67 Bidang ini tidak lagi mereferen sikan standar.

Nilai untuk bidang ASFF yang disediakan pelanggan setelah mengaktifkan temuan kontrol konsolidasi

Jika Anda mengaktifkan temuan kontrol konsolidasi, Security Hub CSPM menghasilkan satu temuan di seluruh standar dan mengarsipkan temuan asli (temuan terpisah untuk setiap standar).

Pembaruan yang Anda buat untuk temuan asli dengan menggunakan konsol CSPM Hub Keamanan atau BatchUpdateFindings operasi tidak akan dipertahankan dalam temuan baru. Jika perlu, Anda dapat memulihkan data ini dengan mengacu pada temuan yang diarsipkan. Untuk meninjau temuan yang diarsipkan, Anda dapat menggunakan halaman Temuan di konsol CSPM Security Hub dan

mengatur filter status rekaman ke ARCHIVED. Atau, Anda dapat menggunakan pen GetFindings goperasian Security Hub CSPM API.

Customer-provided Bidang ASFF	Deskripsi perubahan setelah mengaktifkan temuan kontrol konsolidasi
Kepercayaan	Setel ulang ke keadaan kosong.
Kekritisan	Setel ulang ke keadaan kosong.
Catatan	Setel ulang ke keadaan kosong.
RelatedFindings	Setel ulang ke keadaan kosong.
Kepelikan	Tingkat keparahan default temuan (cocok dengan tingkat keparahan kontrol).
Tipe	Setel ulang ke nilai standar-agnostik.
UserDefinedFields	Setel ulang ke keadaan kosong.
VerificationState	Setel ulang ke keadaan kosong.
Alur kerja	Temuan baru yang gagal memiliki nilai default`NEW`. Temuan baru yang lulus memiliki nilai default`RESOLVED`.

ID Generator sebelum dan sesudah mengaktifkan temuan kontrol konsolidasi

Tabel berikut mencantumkan perubahan pada nilai ID generator untuk kontrol saat Anda mengaktifkan temuan kontrol konsolidasi. Perubahan ini berlaku untuk kontrol yang didukung CSPM Security Hub per 15 Februari 2023.

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.1	keamanan- control/CloudWatch .1

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.10	keamanan- control/IAM .16
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.11	keamanan- control/IAM .17
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.12	keamanan- control/IAM .4
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.13	keamanan- control/IAM .9
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.14	keamanan- control/IAM .6
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.16	keamanan- control/IAM .2
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.2	keamanan- control/IAM .5
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.20	keamanan- control/IAM .18
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.22	keamanan- control/IAM .1
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.3	keamanan- control/IAM .8
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.4	keamanan- control/IAM .3
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.5	keamanan- control/IAM .11

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.6	keamanan- control/IAM .12
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.7	keamanan- control/IAM .13
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.8	keamanan- control/IAM .14
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/1.9	keamanan- control/IAM .15
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.1	keamanan- control/CloudTrail .1
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.2	keamanan- control/CloudTrail .4
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.3	keamanan- control/CloudTrail .6
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.4	keamanan- control/CloudTrail .5
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.5	keamanan- control/Config .1
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.6	keamanan- control/CloudTrail .7
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.7	keamanan- control/CloudTrail .2
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.8	keamanan- control/KMS .4

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/2.9	keamanan- control/EC2 .6
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.1	keamanan- control/CloudWatch .2
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.2	keamanan- control/CloudWatch .3
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.3	keamanan- control/CloudWatch .1
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.4	keamanan- control/CloudWatch .4
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.5	keamanan- control/CloudWatch .5
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.6	keamanan- control/CloudWatch .6
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.7	keamanan- control/CloudWatch .7
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.8	keamanan- control/CloudWatch .8
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.9	keamanan- control/CloudWatch .9
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.10	keamanan- control/CloudWatch .10
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.11	keamanan- control/CloudWatch .11

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.12	keamanan- control/CloudWatch .12
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.13	keamanan- control/CloudWatch .13
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/3.14	keamanan- control/CloudWatch .14
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/4.1	keamanan- control/EC2 .13
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/4.2	keamanan- control/EC2 .14
arn:aws:securityhub::: -aws-fondasi- /1.2. ruleset/cis benchmark/v 0/rule/4.3	keamanan- control/EC2 .2
cis-aws-fondasi- /1.4. benchmark/v 0/1.10	keamanan- control/IAM .5
cis-aws-fondasi- /1.4. benchmark/v 0/1.14	keamanan- control/IAM .3
cis-aws-fondasi- /1.4. benchmark/v 0/1.16	keamanan- control/IAM .1
cis-aws-fondasi- /1.4. benchmark/v 0/1.17	keamanan- control/IAM .18
cis-aws-fondasi- /1.4. benchmark/v 0/1.4	keamanan- control/IAM .4
cis-aws-fondasi- /1.4. benchmark/v 0/1.5	keamanan- control/IAM .9
cis-aws-fondasi- /1.4. benchmark/v 0/1.6	keamanan- control/IAM .6
cis-aws-fondasi- /1.4. benchmark/v 0/1.7	keamanan- control/CloudWatch .1
cis-aws-fondasi- /1.4. benchmark/v 0/1.8	keamanan- control/IAM .15
cis-aws-fondasi- /1.4. benchmark/v 0/1.9	keamanan- control/IAM .16

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
cis-aws-fondasi- /1.4. benchmark/v 0/2.1.2	keamanan- control/S3 .5
cis-aws-fondasi- /1.4. benchmark/v 0/2.1.5.1	keamanan- control/S3 .1
cis-aws-fondasi- /1.4. benchmark/v 0/2.1.5.2	keamanan- control/S3 .8
cis-aws-fondasi- /1.4. benchmark/v 0/2.2.1	keamanan- control/EC2 .7
cis-aws-fondasi- /1.4. benchmark/v 0/2.3.1	keamanan- control/RDS .3
cis-aws-fondasi- /1.4. benchmark/v 0/3.1	keamanan- control/CloudTrail .1
cis-aws-fondasi- /1.4. benchmark/v 0/3.2	keamanan- control/CloudTrail .4
cis-aws-fondasi- /1.4. benchmark/v 0/3.4	keamanan- control/CloudTrail .5
cis-aws-fondasi- /1.4. benchmark/v 0/3.5	keamanan- control/Config .1
cis-aws-fondasi- /1.4. benchmark/v 0/3.6	keamanan- control/S3 .9
cis-aws-fondasi- /1.4. benchmark/v 0/3.7	keamanan- control/CloudTrail .2
cis-aws-fondasi- /1.4. benchmark/v 0/3.8	keamanan- control/KMS .4
cis-aws-fondasi- /1.4. benchmark/v 0/3.9	keamanan- control/EC2 .6
cis-aws-fondasi- /1.4. benchmark/v 0/4.3	keamanan- control/CloudWatch .1
cis-aws-fondasi- /1.4. benchmark/v 0/4.4	keamanan- control/CloudWatch .4
cis-aws-fondasi- /1.4. benchmark/v 0/4.5	keamanan- control/CloudWatch .5
cis-aws-fondasi- /1.4. benchmark/v 0/4.6	keamanan- control/CloudWatch .6
cis-aws-fondasi- /1.4. benchmark/v 0/4.7	keamanan- control/CloudWatch .7
cis-aws-fondasi- /1.4. benchmark/v 0/4.8	keamanan- control/CloudWatch .8
cis-aws-fondasi- /1.4. benchmark/v 0/4.9	keamanan- control/CloudWatch .9

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
cis-aws-fondasi- /1.4. benchmark/v 0/4.10	keamanan- control/CloudWatch .10
cis-aws-fondasi- /1.4. benchmark/v 0/4.11	keamanan- control/CloudWatch .11
cis-aws-fondasi- /1.4. benchmark/v 0/4.12	keamanan- control/CloudWatch .12
cis-aws-fondasi- /1.4. benchmark/v 0/4.13	keamanan- control/CloudWatch .13
cis-aws-fondasi- /1.4. benchmark/v 0/4.14	keamanan- control/CloudWatch .14
cis-aws-fondasi- /1.4. benchmark/v 0/5.1	keamanan- control/EC2 .21
cis-aws-fondasi- /1.4. benchmark/v 0/5.3	keamanan- control/EC2 .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Account.1	keamanan- control/Account .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ACM.1	keamanan- control/ACM .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/APIGateway.1	keamanan- control/APIGateway .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/APIGateway.2	keamanan- control/APIGateway .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/APIGateway.3	keamanan- control/APIGateway .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/APIGateway.4	keamanan- control/APIGateway .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/APIGateway.5	keamanan- control/APIGateway .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/APIGateway.8	keamanan- control/APIGateway .8

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/APIGateway.9	keamanan- control/APIGateway .9
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/AutoScaling.1	keamanan- control/AutoScaling .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/AutoScaling.2	keamanan- control/AutoScaling .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/AutoScaling.3	keamanan- control/AutoScaling .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Autoscaling.5	keamanan- control/Autoscaling .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/AutoScaling.6	keamanan- control/AutoScaling .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/AutoScaling.9	keamanan- control/AutoScaling .9
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.1	keamanan- control/CloudFront .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.3	keamanan- control/CloudFront .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.4	keamanan- control/CloudFront .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.5	keamanan- control/CloudFront .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.6	keamanan- control/CloudFront .6

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.7	keamanan- control/CloudFront .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.8	keamanan- control/CloudFront .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.9	keamanan- control/CloudFront .9
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.10	keamanan- control/CloudFront .10
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudFront.12	keamanan- control/CloudFront .12
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudTrail.1	keamanan- control/CloudTrail .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudTrail.2	keamanan- control/CloudTrail .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudTrail.4	keamanan- control/CloudTrail .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CloudTrail.5	keamanan- control/CloudTrail .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CodeBuild.1	keamanan- control/CodeBuild .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CodeBuild.2	keamanan- control/CodeBuild .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CodeBuild.3	keamanan- control/CodeBuild .3

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/CodeBuild.4	keamanan- control/CodeBuild .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Config.1	keamanan- control/Config .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/DMS.1	keamanan- control/DMS .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/DynamoDB.1	keamanan- control/DynamoDB .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/DynamoDB.2	keamanan- control/DynamoDB .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/DynamoDB.3	keamanan- control/DynamoDB .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.1	keamanan- control/EC2 .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.3	keamanan- control/EC2 .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.4	keamanan- control/EC2 .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.6	keamanan- control/EC2 .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.7	keamanan- control/EC2 .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.8	keamanan- control/EC2 .8

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.9	keamanan- control/EC2 .9
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.10	keamanan- control/EC2 .10
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.15	keamanan- control/EC2 .15
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.16	keamanan- control/EC2 .16
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.17	keamanan- control/EC2 .17
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.18	keamanan- control/EC2 .18
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.19	keamanan- control/EC2 .19
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.2	keamanan- control/EC2 .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.20	keamanan- control/EC2 .20
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.21	keamanan- control/EC2 .21
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.23	keamanan- control/EC2 .23
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.24	keamanan- control/EC2 .24

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EC2.25	keamanan- control/EC2 .25
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECR.1	keamanan- control/ECR .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECR.2	keamanan- control/ECR .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECR.3	keamanan- control/ECR .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECS.10	keamanan- control/ECS .10
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECS.12	keamanan- control/ECS .12
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECS.2	keamanan- control/ECS .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECS.3	keamanan- control/ECS .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECS.4	keamanan- control/ECS .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECS.5	keamanan- control/ECS .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ECS.8	keamanan- control/ECS .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EFS.1	keamanan- control/EFS .1

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EFS.2	keamanan- control/EFS .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EFS.3	keamanan- control/EFS .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EFS.4	keamanan- control/EFS .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EKS.2	keamanan- control/EKS .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ElasticBeanstalk.1	keamanan- control/ElasticBeanstalk .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ElasticBeanstalk.2	keamanan- control/ElasticBeanstalk .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELBv2.1	keamanan- control/ELB .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.2	keamanan- control/ELB .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.3	keamanan- control/ELB .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.4	keamanan- control/ELB .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.5	keamanan- control/ELB .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.6	keamanan- control/ELB .6

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.7	keamanan- control/ELB .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.8	keamanan- control/ELB .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.9	keamanan- control/ELB .9
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.10	keamanan- control/ELB .10
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.11	keamanan- control/ELB .11
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.12	keamanan- control/ELB .12
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.13	keamanan- control/ELB .13
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ELB.14	keamanan- control/ELB .14
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/EMR.1	keamanan- control/EMR .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.1	keamanan- control/ES .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.2	keamanan- control/ES .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.3	keamanan- control/ES .3

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.4	keamanan- control/ES .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.5	keamanan- control/ES .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.6	keamanan- control/ES .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.7	keamanan- control/ES .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/ES.8	keamanan- control/ES .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/GuardDuty.1	keamanan- control/GuardDuty .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.1	keamanan- control/IAM .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.2	keamanan- control/IAM .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.21	keamanan- control/IAM .21
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.3	keamanan- control/IAM .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.4	keamanan- control/IAM .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.5	keamanan- control/IAM .5

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.6	keamanan- control/IAM .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.7	keamanan- control/IAM .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/IAM.8	keamanan- control/IAM .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Kinesis.1	keamanan- control/Kinesis .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/KMS.1	keamanan- control/KMS .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/KMS.2	keamanan- control/KMS .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/KMS.3	keamanan- control/KMS .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Lambda.1	keamanan- control/Lambda .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Lambda.2	keamanan- control/Lambda .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Lambda.5	keamanan- control/Lambda .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/NetworkFirewall.3	keamanan- control/NetworkFirewall .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/NetworkFirewall.4	keamanan- control/NetworkFirewall .4

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/NetworkFirewall.5	keamanan- control/NetworkFirewall .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/NetworkFirewall.6	keamanan- control/NetworkFirewall .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.1	keamanan- control/Opensearch .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.2	keamanan- control/Opensearch .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.3	keamanan- control/Opensearch .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.4	keamanan- control/Opensearch .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.5	keamanan- control/Opensearch .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.6	keamanan- control/Opensearch .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.7	keamanan- control/Opensearch .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Opensearch.8	keamanan- control/Opensearch .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.1	keamanan- control/RDS .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.10	keamanan- control/RDS .10

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.11	keamanan- control/RDS .11
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.12	keamanan- control/RDS .12
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.13	keamanan- control/RDS .13
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.14	keamanan- control/RDS .14
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.15	keamanan- control/RDS .15
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.16	keamanan- control/RDS .16
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.17	keamanan- control/RDS .17
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.19	keamanan- control/RDS .19
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.2	keamanan- control/RDS .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.20	keamanan- control/RDS .20
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.21	keamanan- control/RDS .21
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.22	keamanan- control/RDS .22

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.23	keamanan- control/RDS .23
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.24	keamanan- control/RDS .24
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.25	keamanan- control/RDS .25
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.3	keamanan- control/RDS .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.4	keamanan- control/RDS .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.5	keamanan- control/RDS .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.6	keamanan- control/RDS .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.7	keamanan- control/RDS .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.8	keamanan- control/RDS .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/RDS.9	keamanan- control/RDS .9
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Redshift.1	keamanan- control/Redshift .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Redshift.2	keamanan- control/Redshift .2

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Redshift.3	keamanan- control/Redshift .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Redshift.4	keamanan- control/Redshift .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Redshift.6	keamanan- control/Redshift .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Redshift.7	keamanan- control/Redshift .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/Redshift.8	keamanan- control/Redshift .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.1	keamanan- control/S3 .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.12	keamanan- control/S3 .12
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.13	keamanan- control/S3 .13
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.2	keamanan- control/S3 .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.3	keamanan- control/S3 .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.5	keamanan- control/S3 .5
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.6	keamanan- control/S3 .6

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.8	keamanan- control/S3 .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/S3.9	keamanan- control/S3 .9
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SageMaker.1	keamanan- control/SageMaker .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SageMaker.2	keamanan- control/SageMaker .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SageMaker.3	keamanan- control/SageMaker .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SecretsManager.1	keamanan- control/SecretsManager .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SecretsManager.2	keamanan- control/SecretsManager .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SecretsManager.3	keamanan- control/SecretsManager .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SecretsManager.4	keamanan- control/SecretsManager .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SQS.1	keamanan- control/SQS .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SSM.1	keamanan- control/SSM .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SSM.2	keamanan- control/SSM .2

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SSM.3	keamanan- control/SSM .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/SSM.4	keamanan- control/SSM .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.1	keamanan- control/WAF .1
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.2	keamanan- control/WAF .2
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.3	keamanan- control/WAF .3
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.4	keamanan- control/WAF .4
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.6	keamanan- control/WAF .6
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.7	keamanan- control/WAF .7
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.8	keamanan- control/WAF .8
aws-dasar-keamanan-terbaik- /1.0. practices/v 0/WAF.10	keamanan- control/WAF .10
pci- dss/v /3.2. 1/PCI. AutoScaling.1	keamanan- control/AutoScaling .1
pci- dss/v /3.2. 1/PCI. CloudTrail.1	keamanan- control/CloudTrail .2
pci- dss/v /3.2. 1/PCI. CloudTrail.2	keamanan- control/CloudTrail .3
pci- dss/v /3.2. 1/PCI. CloudTrail.3	keamanan- control/CloudTrail .4

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
pci- dss/v /3.2. 1/PCI. CloudTrail.4	keamanan- control/CloudTrail .5
pci- dss/v /3.2. 1/PCI. CodeBuild.1	keamanan- control/CodeBuild .1
pci- dss/v /3.2. 1/PCI. CodeBuild.2	keamanan- control/CodeBuild .2
pci- dss/v /3.2. 1/PCI. Config.1	keamanan- control/Config .1
pci- dss/v /3.2. 1/PCI. CW.1	keamanan- control/CloudWatch .1
pci- dss/v /3.2. 1/PCI. DMS.1	keamanan- control/DMS .1
pci- dss/v /3.2. 1/PCI. EC2.1	keamanan- control/EC2 .1
pci- dss/v /3.2. 1/PCI. EC2.2	keamanan- control/EC2 .2
pci- dss/v /3.2. 1/PCI. EC2.4	keamanan- control/EC2 .12
pci- dss/v /3.2. 1/PCI. EC2.5	keamanan- control/EC2 .13
pci- dss/v /3.2. 1/PCI. EC2.6	keamanan- control/EC2 .6
pci- dss/v /3.2. 1/PCI. ELBv2.1	keamanan- control/ELB .1
pci- dss/v /3.2. 1/PCI. ES.1	keamanan- control/ES .2
pci- dss/v /3.2. 1/PCI. ES.2	keamanan- control/ES .1
pci- dss/v /3.2. 1/PCI. GuardDuty.1	keamanan- control/GuardDuty .1
pci- dss/v /3.2. 1/PCI. IAM.1	keamanan- control/IAM .4
pci- dss/v /3.2. 1/PCI. IAM.2	keamanan- control/IAM .2
pci- dss/v /3.2. 1/PCI. IAM.3	keamanan- control/IAM .1
pci- dss/v /3.2. 1/PCI. IAM.4	keamanan- control/IAM .6
pci- dss/v /3.2. 1/PCI. IAM.5	keamanan- control/IAM .9

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
pci- dss/v /3.2. 1/PCI. IAM.6	keamanan- control/IAM .19
pci- dss/v /3.2. 1/PCI. IAM.7	keamanan- control/IAM .8
pci- dss/v /3.2. 1/PCI. IAM.8	keamanan- control/IAM .10
pci- dss/v /3.2. 1/PCI. KMS.1	keamanan- control/KMS .4
pci- dss/v /3.2. 1/PCI. Lambda.1	keamanan- control/Lambda .1
pci- dss/v /3.2. 1/PCI. Lambda.2	keamanan- control/Lambda .3
pci- dss/v /3.2. 1/PCI. Opensearch.1	keamanan- control/Opensearch .2
pci- dss/v /3.2. 1/PCI. Opensearch.2	keamanan- control/Opensearch .1
pci- dss/v /3.2. 1/PCI. RDS.1	keamanan- control/RDS .1
pci- dss/v /3.2. 1/PCI. RDS.2	keamanan- control/RDS .2
pci- dss/v /3.2. 1/PCI. Redshift.1	keamanan- control/Redshift .1
pci- dss/v /3.2. 1/PCI. S3.1	keamanan- control/S3 .3
pci- dss/v /3.2. 1/PCI. S3.2	keamanan- control/S3 .2
pci- dss/v /3.2. 1/PCI. S3.3	keamanan- control/S3 .7
pci- dss/v /3.2. 1/PCI. S3.5	keamanan- control/S3 .5
pci- dss/v /3.2. 1/PCI. S3.6	keamanan- control/S3 .1
pci- dss/v /3.2. 1/PCI. SageMaker.1	keamanan- control/SageMaker .1
pci- dss/v /3.2. 1/PCI. SSM.1	keamanan- control/SSM .2
pci- dss/v /3.2. 1/PCI. SSM.2	keamanan- control/SSM .3
pci- dss/v /3.2. 1/PCI. SSM.3	keamanan- control/SSM .1

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ACM.1	keamanan- control/ACM .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ APIGateway.1	keamanan- control/APIGateway .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ APIGateway.2	keamanan- control/APIGateway .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ APIGateway.3	keamanan- control/APIGateway .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ APIGateway.4	keamanan- control/APIGateway .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ APIGateway.5	keamanan- control/APIGateway .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ AutoScaling.1	keamanan- control/AutoScaling .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ AutoScaling.2	keamanan- control/AutoScaling .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ AutoScaling.3	keamanan- control/AutoScaling .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ AutoScaling.4	keamanan- control/AutoScaling .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Autoscaling.5	keamanan- control/Autoscaling .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ AutoScaling.6	keamanan- control/AutoScaling .6

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ AutoScaling.9	keamanan- control/AutoScaling .9
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CloudTrail.1	keamanan- control/CloudTrail .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CloudTrail.2	keamanan- control/CloudTrail .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CloudTrail.4	keamanan- control/CloudTrail .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CloudTrail.5	keamanan- control/CloudTrail .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CodeBuild.1	keamanan- control/CodeBuild .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CodeBuild.2	keamanan- control/CodeBuild .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CodeBuild.4	keamanan- control/CodeBuild .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ CodeBuild.5	keamanan- control/CodeBuild .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ DMS.1	keamanan- control/DMS .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ DynamoDB.1	keamanan- control/DynamoDB .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ DynamoDB.2	keamanan- control/DynamoDB .2

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.1	keamanan- control/EC2 .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.2	keamanan- control/EC2 .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.3	keamanan- control/EC2 .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.4	keamanan- control/EC2 .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.6	keamanan- control/EC2 .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.7	keamanan- control/EC2 .7
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.8	keamanan- control/EC2 .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.9	keamanan- control/EC2 .9
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.10	keamanan- control/EC2 .10
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.15	keamanan- control/EC2 .15
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.16	keamanan- control/EC2 .16
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.17	keamanan- control/EC2 .17

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.18	keamanan- control/EC2 .18
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.19	keamanan- control/EC2 .19
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.20	keamanan- control/EC2 .20
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.21	keamanan- control/EC2 .21
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EC2.22	keamanan- control/EC2 .22
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECR.1	keamanan- control/ECR .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECR.2	keamanan- control/ECR .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECR.3	keamanan- control/ECR .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECS.2	keamanan- control/ECS .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECS.3	keamanan- control/ECS .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECS.4	keamanan- control/ECS .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECS.5	keamanan- control/ECS .5

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECS.8	keamanan- control/ECS .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECS.10	keamanan- control/ECS .10
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ECS.12	keamanan- control/ECS .12
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EFS.1	keamanan- control/EFS .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EFS.2	keamanan- control/EFS .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EFS.3	keamanan- control/EFS .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EFS.4	keamanan- control/EFS .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EKS.2	keamanan- control/EKS .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.2	keamanan- control/ELB .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.3	keamanan- control/ELB .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.4	keamanan- control/ELB .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.5	keamanan- control/ELB .5

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.6	keamanan- control/ELB .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.7	keamanan- control/ELB .7
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.8	keamanan- control/ELB .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.9	keamanan- control/ELB .9
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.10	keamanan- control/ELB .10
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.12	keamanan- control/ELB .12
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.13	keamanan- control/ELB .13
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELB.14	keamanan- control/ELB .14
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ELBv2.1	keamanan- control/ELBv2 .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ EMR.1	keamanan- control/EMR .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.1	keamanan- control/ES .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.2	keamanan- control/ES .2

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.3	keamanan- control/ES .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.4	keamanan- control/ES .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.5	keamanan- control/ES .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.6	keamanan- control/ES .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.7	keamanan- control/ES .7
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ES.8	keamanan- control/ES .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ElasticBeanstalk.1	keamanan- control/ElasticBeanstalk .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ ElasticBeanstalk.2	keamanan- control/ElasticBeanstalk .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ GuardDuty.1	keamanan- control/GuardDuty .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.1	keamanan- control/IAM .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.2	keamanan- control/IAM .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.3	keamanan- control/IAM .3

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.4	keamanan- control/IAM .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.5	keamanan- control/IAM .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.6	keamanan- control/IAM .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.7	keamanan- control/IAM .7
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.8	keamanan- control/IAM .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ IAM.21	keamanan- control/IAM .21
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Kinesis.1	keamanan- control/Kinesis .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ KMS.1	keamanan- control/KMS .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ KMS.2	keamanan- control/KMS .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ KMS.3	keamanan- control/KMS .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Lambda.1	keamanan- control/Lambda .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Lambda.2	keamanan- control/Lambda .2

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Lambda.5	keamanan- control/Lambda .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ NetworkFirewall.3	keamanan- control/NetworkFirewall .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ NetworkFirewall.4	keamanan- control/NetworkFirewall .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ NetworkFirewall.5	keamanan- control/NetworkFirewall .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ NetworkFirewall.6	keamanan- control/NetworkFirewall .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.1	keamanan- control/Opensearch .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.2	keamanan- control/Opensearch .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.3	keamanan- control/Opensearch .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.4	keamanan- control/Opensearch .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.5	keamanan- control/Opensearch .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.6	keamanan- control/Opensearch .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.7	keamanan- control/Opensearch .7

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Opensearch.8	keamanan- control/Opensearch .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.1	keamanan- control/RDS .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.2	keamanan- control/RDS .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.3	keamanan- control/RDS .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.4	keamanan- control/RDS .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.5	keamanan- control/RDS .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.6	keamanan- control/RDS .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.8	keamanan- control/RDS .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.9	keamanan- control/RDS .9
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.10	keamanan- control/RDS .10
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.11	keamanan- control/RDS .11
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.13	keamanan- control/RDS .13

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.17	keamanan- control/RDS .17
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.19	keamanan- control/RDS .19
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.20	keamanan- control/RDS .20
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.21	keamanan- control/RDS .21
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.22	keamanan- control/RDS .22
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.23	keamanan- control/RDS .23
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ RDS.25	keamanan- control/RDS .25
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Redshift.1	keamanan- control/Redshift .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Redshift.2	keamanan- control/Redshift .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Redshift.4	keamanan- control/Redshift .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Redshift.6	keamanan- control/Redshift .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Redshift.7	keamanan- control/Redshift .7

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ Redshift.8	keamanan- control/Redshift .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.1	keamanan- control/S3 .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.2	keamanan- control/S3 .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.3	keamanan- control/S3 .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.5	keamanan- control/S3 .5
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.6	keamanan- control/S3 .6
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.8	keamanan- control/S3 .8
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.9	keamanan- control/S3 .9
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.12	keamanan- control/S3 .12
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ S3.13	keamanan- control/S3 .13
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SageMaker.1	keamanan- control/SageMaker .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SecretsManager.1	keamanan- control/SecretsManager .1

GeneratorID sebelum mengaktifkan temuan kontrol konsolidasi	GeneratorID setelah mengaktifkan temuan kontrol konsolidasi
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SecretsManager.2	keamanan- control/SecretsManager .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SecretsManager.3	keamanan- control/SecretsManager .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SecretsManager.4	keamanan- control/SecretsManager .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SQS.1	keamanan- control/SQS .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SSM.1	keamanan- control/SSM .1
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SSM.2	keamanan- control/SSM .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SSM.3	keamanan- control/SSM .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ SSM.4	keamanan- control/SSM .4
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ WAF.2	keamanan- control/WAF .2
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ WAF.3	keamanan- control/WAF .3
layanan-dikelolan-aws-kontrol- /1.0. tower/v 0/ WAF.4	keamanan- control/WAF .4

Bagaimana konsolidasi memengaruhi ID kontrol dan judul

Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi menstandarkan ID kontrol dan judul di seluruh standar. Istilah ID kontrol keamanan dan judul kontrol keamanan mengacu pada nilai-nilai agnostik standar ini.

Konsol Security Hub CSPM menampilkan ID kontrol keamanan standar dan judul kontrol keamanan, terlepas dari apakah temuan kontrol konsolidasi diaktifkan atau dinonaktifkan untuk akun Anda. Namun, temuan Security Hub CSPM berisi judul kontrol khusus standar, untuk PCI DSS dan CIS v1.2.0, jika temuan kontrol konsolidasi dinonaktifkan untuk akun Anda. Selain itu, temuan Security Hub CSPM berisi ID kontrol khusus standar dan ID kontrol keamanan. Untuk contoh bagaimana konsolidasi berdampak pada temuan kontrol, lihatSampel temuan kontrol.

Untuk kontrol yang merupakan bagian dari standar yang AWS Control Tower dikelola layanan, awalan `CT.` dihapus dari ID kontrol dan judul dalam temuan saat temuan kontrol konsolidasi diaktifkan.

Untuk menonaktifkan kontrol keamanan di Security Hub CSPM, Anda harus menonaktifkan semua kontrol standar yang sesuai dengan kontrol keamanan. Tabel berikut menunjukkan pemetaan ID kontrol keamanan dan judul ke ID kontrol khusus standar dan judul. ID dan judul untuk kontrol yang termasuk dalam standar F AWS oundational Security Best Practices (FSBP) sudah standar agnostik. Untuk pemetaan kontrol dengan persyaratan Center for Internet Security (CIS) v3.0.0, lihat. Pemetaan kontrol ke persyaratan CIS di setiap versi Untuk menjalankan skrip Anda sendiri di tabel ini, Anda dapat mengunduhnya sebagai fil e.csv.

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	1.1 Hindari penggunaan pengguna root	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
CIS v1.2.0	1.10 Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
CIS v1.2.0	1.11 Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang	[IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	1.12 Pastikan tidak ada kunci akses pengguna root	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
CIS v1.2.0	1.13 Pastikan MFA diaktifkan untuk pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
CIS v1.2.0	1.14 Pastikan MFA perangkat keras diaktifkan untuk pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
CIS v1.2.0	1.16 Pastikan kebijakan IAM hanya dilampirkan ke grup atau peran	[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
CIS v1.2.0	1.2 Pastikan otentikasi multi-fak tor (MFA) diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
CIS v1.2.0	1.20 Pastikan peran pendukung telah dibuat untuk mengelola insiden dengan Dukungan	[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
CIS v1.2.0	1.22 Pastikan kebijakan IAM yang mengizinkan hak administratif penuh “*: *” tidak dibuat	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
CIS v1.2.0	1.3 Pastikan kredensi yang tidak digunakan selama 90 hari atau lebih dinonaktifkan	[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
CIS v1.2.0	1.4 Pastikan kunci akses diputar setiap 90 hari atau kurang	[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
CIS v1.2.0	1.5 Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf besar	[IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	1.6 Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu huruf kecil	[IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
CIS v1.2.0	1.7 Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu simbol	[IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
CIS v1.2.0	1.8 Pastikan kebijakan kata sandi IAM memerlukan setidaknya satu nomor	[IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
CIS v1.2.0	1.9 Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih	[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
CIS v1.2.0	2.1 Pastikan CloudTrail diaktifkan di semua wilayah	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
CIS v1.2.0	2.2 Pastikan validasi file CloudTrail log diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
CIS v1.2.0	2.3 Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik	[CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
CIS v1.2.0	2.4 Pastikan CloudTrail jalur terintegrasi dengan CloudWatch Log	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	2.5 Pastikan AWS Config diaktifkan	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
CIS v1.2.0	2.6 Pastikan logging akses bucket S3 diaktifkan pada bucket CloudTrail S3	[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
CIS v1.2.0	2.7 Pastikan CloudTrail log dienkripsi saat diam menggunakan KMS CMK	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
CIS v1.2.0	2.8 Pastikan rotasi untuk CMK yang dibuat pelanggan diaktifkan	[KMS.4]AWS KMSrotasi kunci harus diaktifkan
CIS v1.2.0	2.9 Pastikan pencatatan aliran VPC diaktifkan di semua VPC	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
CIS v1.2.0	3.1 Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah	[CloudWatch.2] Pastikan filter metrik log dan alarm ada untuk panggilan API yang tidak sah
CIS v1.2.0	3.10 Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
CIS v1.2.0	3.11 Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
CIS v1.2.0	3.12 Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	3.13 Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
CIS v1.2.0	3.14 Pastikan filter metrik log dan alarm ada untuk perubahan VPC	[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC
CIS v1.2.0	3.2 Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA	[CloudWatch.3] Pastikan filter metrik log dan alarm ada untuk login Konsol Manajemen tanpa MFA
CIS v1.2.0	3.3 Pastikan filter metrik log dan alarm ada untuk penggunaan pengguna root	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
CIS v1.2.0	3.4 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM
CIS v1.2.0	3.5 Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi
CIS v1.2.0	3.6 Pastikan filter metrik log dan alarm ada untuk kegagalan Konsol Manajemen AWS otentikasi	[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi
CIS v1.2.0	3.7 Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan CMK yang dibuat pelanggan	[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan
CIS v1.2.0	3.8 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.2.0	3.9 Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi
CIS v1.2.0	4.1 Pastikan tidak ada grup keamanan yang mengizinkan masuk dari 0.0.0. 0/0 ke port 22	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22
CIS v1.2.0	4.2 Pastikan tidak ada grup keamanan yang mengizinkan masuknya dari 0.0.0. 0/0 ke port 3389	[EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
CIS v1.2.0	4.3 Pastikan grup keamanan default dari setiap VPC membatasi semua lalu lintas	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
CIS v1.4.0	1.10 Pastikan otentikasi multi-fak tor (MFA) diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol	[IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
CIS v1.4.0	1.14 Pastikan kunci akses diputar setiap 90 hari atau kurang	[IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
CIS v1.4.0	1.16 Pastikan kebijakan IAM yang mengizinkan hak administratif penuh “*: *” tidak dilampirkan	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
CIS v1.4.0	1.17 Pastikan peran pendukung telah dibuat untuk mengelola insiden dengan Dukungan	[IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
CIS v1.4.0	1.4 Pastikan tidak ada kunci akses akun pengguna root	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	1.5 Pastikan MFA diaktifkan untuk akun pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root
CIS v1.4.0	1.6 Pastikan MFA perangkat keras diaktifkan untuk akun pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
CIS v1.4.0	1.7 Hilangkan penggunaan pengguna root untuk tugas administratif dan harian	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
CIS v1.4.0	1.8 Pastikan kebijakan kata sandi IAM memerlukan panjang minimum 14 atau lebih	[IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
CIS v1.4.0	1.9 Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi	[IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
CIS v1.4.0	2.1.2 Pastikan Kebijakan S3 Bucket diatur untuk menolak permintaan HTTP	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS
CIS v1.4.0	2.1.5.1 Setelan Akses Publik Blok S3 harus diaktifkan	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
CIS v1.4.0	2.1.5.2 Pengaturan Akses Publik Blok S3 harus diaktifkan pada tingkat bucket	[S3.8] Bucket tujuan umum S3 harus memblokir akses publik
CIS v1.4.0	2.2.1 Pastikan enkripsi volume EBS diaktifkan	[EC2.7] Enkripsi default EBS harus diaktifkan
CIS v1.4.0	2.3.1 Pastikan enkripsi diaktifkan untuk Instans RDS	[RDS.3] Instans RDS DB harus mengaktifkan enkripsi saat istirahat

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	3.1 Pastikan CloudTrail diaktifkan di semua wilayah	[CloudTrail.1] CloudTrail harus diaktifkan dan dikonfigurasi dengan setidaknya satu jejak Multi-wilayah yang mencakup acara manajemen baca dan tulis
CIS v1.4.0	3.2 Pastikan validasi file CloudTrail log diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
CIS v1.4.0	3.4 Pastikan CloudTrail jalur terintegrasi dengan CloudWatch Log	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch
CIS v1.4.0	3.5 Pastikan AWS Config diaktifkan di semua wilayah	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
CIS v1.4.0	3.6 Pastikan logging akses bucket S3 diaktifkan pada bucket CloudTrail S3	[CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
CIS v1.4.0	3.7 Pastikan CloudTrail log dienkripsi saat diam menggunakan KMS CMK	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
CIS v1.4.0	3.8 Pastikan rotasi untuk CMK yang dibuat pelanggan diaktifkan	[KMS.4]AWS KMSrotasi kunci harus diaktifkan
CIS v1.4.0	3.9 Pastikan pencatatan aliran VPC diaktifkan di semua VPC	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
CIS v1.4.0	4.4 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM	[CloudWatch.4] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan IAM

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	4.5 Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi	[CloudWatch.5] Pastikan filter metrik log dan alarm ada untuk perubahan CloudTrail konfigurasi
CIS v1.4.0	4.6 Pastikan filter metrik log dan alarm ada untuk kegagalan Konsol Manajemen AWS otentikasi	[CloudWatch.6] Pastikan filter metrik log dan alarm ada untuk Konsol Manajemen AWS kegagalan otentikasi
CIS v1.4.0	4.7 Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan CMK yang dibuat pelanggan	[CloudWatch.7] Pastikan filter metrik log dan alarm ada untuk menonaktifkan atau menjadwalkan penghapusan kunci yang dikelola pelanggan
CIS v1.4.0	4.8 Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3	[CloudWatch.8] Pastikan filter metrik log dan alarm ada untuk perubahan kebijakan bucket S3
CIS v1.4.0	4.9 Pastikan filter metrik log dan alarm ada untuk perubahan AWS Config konfigurasi	[CloudWatch.9] Pastikan filter metrik log dan alarm ada untuk AWS Config perubahan konfigurasi
CIS v1.4.0	4.10 Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan	[CloudWatch.10] Pastikan filter metrik log dan alarm ada untuk perubahan grup keamanan
CIS v1.4.0	4.11 Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)	[CloudWatch.11] Pastikan filter metrik log dan alarm ada untuk perubahan pada Daftar Kontrol Akses Jaringan (NACL)
CIS v1.4.0	4.12 Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan	[CloudWatch.12] Pastikan filter metrik log dan alarm ada untuk perubahan gateway jaringan

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
CIS v1.4.0	4.13 Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute	[CloudWatch.13] Pastikan filter metrik log dan alarm ada untuk perubahan tabel rute
CIS v1.4.0	4.14 Pastikan filter metrik log dan alarm ada untuk perubahan VPC	[CloudWatch.14] Pastikan filter metrik log dan alarm ada untuk perubahan VPC
CIS v1.4.0	5.1 Pastikan tidak ada ACL Jaringan yang mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh	[EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
CIS v1.4.0	5.3 Pastikan grup keamanan default dari setiap VPC membatasi semua lalu lintas	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
PCI DSS v3.2.1	PCI.AutoScaling.1 Grup penskalaan otomatis yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan penyeimbang beban	[AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
PCI DSS v3.2.1	PCI.CloudTrail.1 CloudTrail log harus dienkripsi saat istirahat menggunakan AWS KMS CMK	[CloudTrail.2] CloudTrail harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	PCI.CloudTrail.2 CloudTrail harus diaktifkan	[CloudTrail.3] Setidaknya satu CloudTrail jejak harus diaktifkan
PCI DSS v3.2.1	PCI.CloudTrail.3 CloudTrail Validasi file log harus diaktifkan	[CloudTrail.4] validasi file CloudTrail log harus diaktifkan
PCI DSS v3.2.1	PCI.CloudTrail.4 CloudTrail jalur harus diintegrasikan dengan Amazon CloudWatch Logs	[CloudTrail.5] CloudTrail jalur harus diintegrasikan dengan Amazon Logs CloudWatch

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI.CodeBuild.1 CodeBuild GitHub atau URL repositori sumber Bitbucket harus menggunakan OAuth	[CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
PCI DSS v3.2.1	PCI.CodeBuild.2 CodeBuild variabel lingkungan proyek tidak boleh mengandung kredenSIAL teks yang jelas	[CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
PCI DSS v3.2.1	PCI.Config.1 AWS Config harus diaktifkan	[Config.1] AWS Config harus diaktifkan dan menggunakan peran terkait layanan untuk perekaman sumber daya
PCI DSS v3.2.1	PCI.CW.1 Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”	[CloudWatch.1] Filter metrik log dan alarm harus ada untuk penggunaan pengguna “root”
PCI DSS v3.2.1	PCI.DMS.1 Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik	[DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
PCI DSS v3.2.1	PCI.EC2.1 Snapshot EBS tidak boleh dipulihkan secara publik	[EC2.1] Snapshot Amazon EBS tidak boleh dikonfigurasi agar dapat dipulihkan secara publik
PCI DSS v3.2.1	PCI.EC2.2 Grup keamanan default VPC harus melarang lalu lintas masuk dan keluar	[EC2.2] Grup keamanan default VPC tidak boleh mengizinkan lalu lintas masuk atau keluar
PCI DSS v3.2.1	PCI.EC2.4 EIP EC2 yang tidak digunakan harus dihapus	[EC2.12] EIP Amazon EC2 yang tidak digunakan harus dihapus
PCI DSS v3.2.1	PCI.EC2.5 Grup keamanan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22	[EC2.13] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 22

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI.EC2.6 Pencatatan aliran VPC harus diaktifkan di semua VPC	[EC2.6] Pencatatan aliran VPC harus diaktifkan di semua VPC
PCI DSS v3.2.1	PCI.ELBv2.1 Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS	[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS
PCI DSS v3.2.1	PCI.ES.1 Domain Elasticsearch harus dalam VPC	[ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik
PCI DSS v3.2.1	PCI.ES.2 Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat	[ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	PCI.GuardDuty.1 GuardDuty harus diaktifkan	[GuardDuty.1] GuardDuty harus diaktifkan
PCI DSS v3.2.1	PCI.IAM.1 Kunci akses pengguna root IAM seharusnya tidak ada	[IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
PCI DSS v3.2.1	PCI.IAM.2 Pengguna IAM seharusnya tidak memiliki kebijakan IAM terlampir	[IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
PCI DSS v3.2.1	PCI.IAM.3 Kebijakan IAM seharusnya tidak mengizinkan hak administratif penuh “*”	[IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
PCI DSS v3.2.1	PCI.IAM.4 Perangkat keras MFA harus diaktifkan untuk pengguna root	[IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
PCI DSS v3.2.1	PCI.IAM.5 Virtual MFA harus diaktifkan untuk pengguna root	[IAM.9] MFA harus diaktifkan untuk pengguna root

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI.IAM.6 MFA harus diaktifkan untuk semua pengguna IAM	[IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
PCI DSS v3.2.1	PCI.IAM.7 KredenSIAL pengguna IAM harus dinonaktifkan jika tidak digunakan dalam jumlah hari yang telah ditentukan sebelumnya	[IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
PCI DSS v3.2.1	PCI.IAM.8 Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat	[IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
PCI DSS v3.2.1	PCI.KMS.1 Rotasi kunci master pelanggan (CMK) harus diaktifkan	[KMS.4]AWS KMSrotasi kunci harus diaktifkan
PCI DSS v3.2.1	PCI.Lambda.1 Fungsi lambda harus melarang akses publik	[Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
PCI DSS v3.2.1	PCI.Lambda.2 Fungsi lambda harus dalam VPC	[Lambda.3] Fungsi lambda harus dalam VPC
PCI DSS v3.2.1	PCI.Opensearch.1 OpenSearch domain harus dalam VPC	[Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
PCI DSS v3.2.1	PCI.Opensearch.2 Snapshot EBS tidak boleh dipulihkan secara publik	[Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
PCI DSS v3.2.1	PCI.RDS.1 Snapshot RDS harus bersifat pribadi	[RDS.1] Snapshot RDS harus bersifat pribadi
PCI DSS v3.2.1	PCI.RDS.2 Instans DB RDS harus melarang akses publik	[RDS.2] Instans DB RDS harus melarang akses publik, sebagaimana ditentukan oleh konfigurasi PubliclyAccessible

Standar	ID kontrol standar dan judul	ID dan judul kontrol keamanan
PCI DSS v3.2.1	PCI.Redshift.1 Cluster Amazon Redshift harus melarang akses publik	[Redshift.1] Cluster Amazon Redshift harus melarang akses publik
PCI DSS v3.2.1	PCI.S3.1 Bucket S3 harus melarang akses tulis publik	[S3.3] Bucket tujuan umum S3 harus memblokir akses tulis publik
PCI DSS v3.2.1	PCI.S3.2 Bucket S3 harus melarang akses baca publik	[S3.2] Bucket tujuan umum S3 harus memblokir akses baca publik
PCI DSS v3.2.1	PCI.S3.3 Bucket S3 harus mengaktifkan replikasi lintas wilayah	[S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
PCI DSS v3.2.1	PCI.S3.5 Bucket S3 harus memerlukan permintaan untuk menggunakan Secure Socket Layer	[S3.5] Bucket tujuan umum S3 harus memerlukan permintaan untuk menggunakan TLS
PCI DSS v3.2.1	PCI.S3.6 Pengaturan Akses Publik Blok S3 harus diaktifkan	[S3.1] Bucket tujuan umum S3 harus mengaktifkan pengaturan akses publik blok
PCI DSS v3.2.1	PCI.SageMaker.1 Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung	[SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
PCI DSS v3.2.1	PCI.SSM.1 Instans EC2 yang dikelola oleh Manajer Sistem harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch	[SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
PCI DSS v3.2.1	PCI.SSM.2 Instans EC2 yang dikelola oleh Manajer Sistem harus memiliki status kepatuhan asosiasi COMPLIANT	[SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
PCI DSS v3.2.1	PCI.SSM.3 Instans EC2 harus dikelola oleh AWS Systems Manager	[SSM.1] Instans Amazon EC2 harus dikelola olehAWS Systems Manager

Memperbarui alur kerja untuk konsolidasi

Jika alur kerja Anda tidak bergantung pada format spesifik bidang apa pun dalam temuan kontrol, tidak ada tindakan yang diperlukan.

Jika alur kerja Anda bergantung pada format spesifik dari satu atau lebih bidang dalam temuan kontrol, seperti yang disebutkan dalam tabel sebelumnya, Anda harus memperbarui alur kerja Anda. Misalnya, Jika Anda membuat EventBridge aturan Amazon yang memicu tindakan untuk ID kontrol tertentu, seperti memanggil AWS Lambda fungsi jika ID kontrol sama dengan CIS 2.7, perbarui aturan yang akan digunakan CloudTrail.2, yang merupakan nilai `Compliance.SecurityControlId` bidang untuk kontrol tersebut.

Jika Anda membuat wawasan khusus yang menggunakan bidang atau nilai yang berubah, perbarui wawasan tersebut untuk menggunakan bidang atau nilai baru.

Atribut ASFF tingkat atas yang diperlukan

Atribut tingkat atas berikut dalam Format Pen AWS emuan Keamanan (ASFF) diperlukan untuk semua temuan di Security Hub CSPM. Untuk informasi selengkapnya tentang atribut ini, lihat AwsSecurityFinding di Referensi API Hub AWS Keamanan.

AwsAccountId

Akun AWS ID yang digunakan temuan tersebut.

Contoh

```
"AwsAccountId": "111111111111"
```

CreatedAt

Menunjukkan kapan potensi masalah keamanan atau peristiwa yang ditangkap oleh temuan dibuat.

Contoh

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Deskripsi

Deskripsi temuan. Bidang ini dapat berupa teks boilerplate nonspesifik atau detail yang spesifik untuk contoh temuan.

Untuk temuan kontrol yang dihasilkan oleh Security Hub CSPM, bidang ini memberikan deskripsi kontrol.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol konsolidasi.

Contoh

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

Pengidentifikasi untuk komponen spesifik solusi (unit logika diskrit) yang menghasilkan temuan.

Untuk temuan kontrol yang dihasilkan oleh Security Hub CSPM, bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol konsolidasi.

Contoh

```
"GeneratorId": "security-control/Config.1"
```

Id

Pengidentifikasi khusus produk untuk temuan. Untuk temuan kontrol yang dihasilkan oleh Security Hub CSPM, bidang ini menyediakan Nama Sumber Daya Amazon (ARN) dari temuan tersebut.

Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol konsolidasi.

Contoh

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

Nama Sumber Daya Amazon (ARN) yang dihasilkan oleh Security Hub CSPM yang secara unik mengidentifikasi produk temuan pihak ketiga setelah produk terdaftar dengan Security Hub CSPM.

Format bidang ini adalah `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*.

- Untuk Layanan AWS itu terintegrasi dengan Security Hub CSPM, `company-id` harus "`aws`“, dan `product-id` harus menjadi nama layanan AWS publik. Karena AWS produk dan layanan tidak

terkait dengan akun, `account-id` bagian ARN kosong. Layanan AWS yang belum terintegrasi dengan Security Hub CSPM dianggap produk pihak ketiga.

- Untuk produk publik, `company-id` dan `product-id` harus menjadi nilai ID yang ditentukan pada saat pendaftaran.
- Untuk produk pribadi, `company-id` harus ID akun. Harus `product-id` berupa kata yang dicadangkan “default” atau ID yang ditentukan pada saat pendaftaran.

Contoh

```
// Private ARN
    "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/
default"

// Public ARN
    "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
    "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-
pro"
```

Sumber daya

`Resources`Array objek menyediakan satu set tipe data sumber daya yang menggambarkan AWS sumber daya yang mengacu pada temuan. Untuk detail tentang bidang yang mungkin berisi `Resources` objek, termasuk bidang mana yang diperlukan, lihat Resource di Referensi API Hub AWS Keamanan. Untuk contoh `Resources` objek secara spesifik Layanan AWS, lihatSumber daya Objek ASFF.

Contoh

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
```

```
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
                                    "OffsetRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                     },
                                    "LineRange": {
                                        "Start": 1,
                                        "End": 100,
                                        "StartColumn": 10
                                    }
                                }
                            ]
                        }
                    },
```

```
                    {
                        "Count": 2229,
                        "Type": "URL",
                        "Occurrences": {
                           "LineRanges": [
                               {
                                   "Start": 1,
                                   "End": 13
                               }
                           ]
                        }
                    },
                    {
                        "Count": 13826,
                        "Type": "NameDetection",
                        "Occurrences": {
                            "Records": [
                                {
                                    "RecordIndex": 1,
                                    "JsonPath": "$.ssn.value"
                                }
                            ]
                        }
                    },
                    {
                        "Count": 32,
                        "Type": "AddressDetection"
                    }
                ],
                "TotalCount": 32
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2
                }
            ],
            "TotalCount": 2
        }
    }
},
```

```
 "Type": "AwsEc2Instance",
 "Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
 "Partition": "aws",
 "Region": "us-west-2",
 "ResourceRole": "Target",
 "Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
 },
 "Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IpV4Addresses": ["1.1.1.1"],
  "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "enabled",
   "HttpPutResponseHopLimit": 1,
   "HttpTokens": "optional",
   "InstanceMetadataTags": "disabled"
  }
 },
  "NetworkInterfaces": [
  {
   "NetworkInterfaceId": "eni-e5aa89a3"
  }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIpv6"
 }

]
```

SchemaVersion

Versi skema yang diformat temuan. Nilai bidang ini harus merupakan salah satu versi yang diterbitkan secara resmi yang diidentifikasi oleh AWS. Dalam rilis saat ini, versi skema AWS Security Finding Format adalah`2018-10-08`.

Contoh

```
"SchemaVersion": "2018-10-08"
```

Kepelikan

Mendefinisikan pentingnya sebuah temuan. Untuk detail tentang objek ini, lihat `Severity` di Refer AWS Security Hub ensi API.

`Severity`merupakan objek tingkat atas dalam temuan dan bersarang di bawah objek. `FindingProviderFields`

Nilai `Severity` objek tingkat atas untuk temuan harus diperbarui hanya dengan menggunakan `BatchUpdateFindings` API.

Untuk memberikan informasi tingkat keparahan, penyedia pencari harus memperbarui `Severity` objek di bawah `FindingProviderFields` saat membuat permintaan `BatchImportFindings` API.
Jika `BatchImportFindings` permintaan untuk temuan baru hanya menyediakan `Label` atau hanya menyediakan`Normalized`, Security Hub CSPM secara otomatis mengisi nilai bidang lainnya. `OriginalBid Product` ang dan juga dapat diisi.

Jika `Finding.Severity` objek tingkat atas ada tetapi tidak `Finding.FindingProviderFields` ada, Security Hub CSPM membuat `FindingProviderFields.Severity` objek dan menyalin keseluruhan `Finding.Severity object` ke dalamnya. Ini memastikan bahwa detail asli yang disediakan penyedia dipertahankan dalam `FindingProviderFields.Severity` struktur, bahkan jika `Severity` objek tingkat atas diganti.

Tingkat keparahan temuan tidak mempertimbangkan kekritisan aset yang terlibat atau sumber daya yang mendasarinya. Kekritisan didefinisikan sebagai tingkat kepentingan sumber daya yang terkait dengan temuan. Misalnya, sumber daya yang terkait dengan aplikasi kritis misi memiliki kekritisan yang lebih tinggi daripada sumber daya yang terkait dengan pengujian nonproduksi. Untuk menangkap informasi tentang kekritisan sumber daya, gunakan `Criticality` bidang.

Kami merekomendasikan menggunakan panduan berikut saat menerjemahkan skor tingkat keparahan asli temuan ke nilai `Severity.Label` dalam ASFF.

- `INFORMATIONAL`Kategori ini dapat mencakup temuan untuk`PASSED`,`WARNING`, atau `NOT AVAILABLE` cek atau identifikasi data sensitif.

- `LOW`Temuan yang dapat menghasilkan kompromi di masa depan. Misalnya, kategori ini dapat mencakup kerentanan, kelemahan konfigurasi, dan kata sandi yang terbuka.
- `MEDIUM`Temuan yang menunjukkan kompromi aktif, tetapi tidak ada indikasi bahwa musuh menyelesaikan tujuan mereka. Misalnya, kategori ini dapat mencakup aktivitas malware, aktivitas peretasan, dan deteksi perilaku yang tidak biasa.
- `HIGH`atau `CRITICAL` — Temuan yang menunjukkan bahwa musuh menyelesaikan tujuan mereka, seperti kehilangan data aktif atau kompromi atau penolakan layanan.

Contoh

```
"Severity": {
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

judul

Judul temuan. Bidang ini dapat berisi teks boilerplate nonspesifik atau detail yang spesifik untuk contoh temuan ini.

Untuk temuan kontrol, bidang ini memberikan judul kontrol. Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol konsolidasi.

Contoh

```
"Title": "AWS Config should be enabled"
```

Tipe

Satu atau lebih jenis temuan dalam format *namespace*/*category*/*classifier* yang mengklasifikasikan temuan. Bidang ini tidak mereferensikan standar jika Anda mengaktifkan temuan kontrol konsolidasi.

`Types`harus diperbarui hanya dengan menggunakan `BatchUpdateFindings` API.

Menemukan penyedia yang ingin memberikan nilai untuk `Types` harus menggunakan `Types` atribut di bawah `FindingProviderFields`.

Dalam daftar berikut, peluru tingkat atas adalah ruang nama, peluru tingkat kedua adalah kategori, dan peluru tingkat ketiga adalah pengklasifikasi. Sebaiknya penyedia pencari menggunakan ruang nama yang ditentukan untuk membantu mengurutkan dan mengelompokkan temuan. Kategori dan pengklasifikasi yang ditentukan juga dapat digunakan, tetapi tidak diperlukan. Hanya namespace Pemeriksaan Perangkat Lunak dan Konfigurasi yang telah menentukan pengklasifikasi.

Anda dapat menentukan jalur parSIAL untuk namespace/category /classfier. Misalnya, jenis temuan berikut semuanya valid:

- TTP
- TTPs/Defense Penghindaran
- TTPs/Defense Evasion/CloudTrailStopped

Kategori taktik, teknik, dan prosedur (TTP) dalam daftar berikut selaras dengan MITRE ATT&CK MatrixTM. Namespace Perilaku Tidak Biasa mencerminkan perilaku umum yang tidak biasa, seperti anomali statistik umum, dan tidak selaras dengan TTP tertentu. Namun, Anda dapat mengklasifikasikan temuan dengan tipe temuan Perilaku Tidak Biasa dan TTP.

Daftar ruang nama, kategori, dan pengklasifikasi:

- Pemeriksaan Perangkat Lunak dan Konfigurasi
  - Kerentanan
    - CVE
  - AWS Praktik Terbaik Keamanan
    - Keterjangkauan Jaringan
    - Analisis Perilaku Waktu Aktif
  - Standar Industri dan Peraturan
    - AWS Praktik Terbaik Keamanan Dasar
    - Tolok Ukur Pengerasan Host CIS
    - Tolok U AWS kur Yayasan CIS
    - PCI-DSS
    - Kontrol Aliansi Keamanan Cloud
    - Kontrol ISO 90001
    - Kontrol ISO 27001
    - Kontrol ISO 27017

    - Kontrol ISO 27018
    - SOC 1
    - SOC 2
    - Kontrol HIPAA (AS)
    - Kontrol NIST 800-53 (AS)
    - Kontrol CSF NIST (AS)
    - Kontrol IRAP (Australia)
    - K-ISMS Kontrol (Korea)
    - Kontrol MTCS (Singapura)
    - Kontrol FISC (Jepang)
    - Kontrol Undang-Undang Nomor Saya (Jepang)
    - ENS Controls (Spanyol)
    - Kontrol Cyber Essentials Plus (Inggris)
    - G-Cloud Kontrol (Inggris)
    - Kontrol C5 (Jerman)
    - IT-Grundschutz Kontrol (Jerman)
    - Kontrol GDPR (Eropa)
    - Kontrol TISAX (Eropa)
  - Manajemen Patch
- TTP
  - Akses Awal
  - Eksekusi
  - Tetap
  - Eskalasi hak istimewa
  - Penghindaran Pertahanan
  - Akses Kredensi
  - Penemuan
  - Gerakan Lateral
  - Koleksi
  - Perintah dan Kontrol

- Efek
  - Paparan Data
  - Ekfiltrasi Data
  - Penghancuran Data
  - Penolakan Layanan
  - Konsumsi Sumber Daya
- Perilaku yang Tidak Biasa
  - Aplikasi
  - Aliran Jaringan
  - Alamat IP
  - Pengguna
  - VM
  - Kontainer
  - Nirserver
  - Proses
  - Basis Data
  - Data
- Identifikasi Data Sensitif
  - PII
  - Kata Sandi
  - Legal
  - Keuangan
  - Keamanan
  - Bisnis

Contoh

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

Menunjukkan kapan penyedia temuan terakhir memperbarui catatan temuan.

Stempel waktu ini mencerminkan waktu ketika catatan temuan terakhir atau terbaru diperbarui. Akibatnya, ini dapat berbeda dari stem `LastObservedAt` pel waktu, yang mencerminkan kapan peristiwa atau kerentanan terakhir atau terakhir diamati.

Saat Anda memperbarui catatan temuan, Anda harus memperbarui stempel waktu ini ke stempel waktu saat ini. Setelah membuat catatan temuan, cap `CreatedAt` waktu `UpdatedAt` dan stempel harus sama. Setelah pembaruan pada catatan temuan, nilai bidang ini harus lebih baru daripada semua nilai sebelumnya yang dikandungnya.

Perhatikan bahwa `UpdatedAt` tidak dapat diperbarui dengan menggunakan `BatchUpdateFindings` operasi. Anda dapat memperbaruinya hanya dengan menggunakan `BatchImportFindings` operasi.

Contoh

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Atribut ASFF tingkat atas opsional

Atribut tingkat atas berikut dalam Format Penem AWS uan Keamanan (ASFF) bersifat opsional untuk temuan di Security Hub CSPM. Untuk informasi selengkapnya tentang atribut ini, lihat AwsSecurityFinding di Referensi API Hub AWS Keamanan.

Tindakan

Ob `Action` jek memberikan rincian tentang tindakan yang mempengaruhi atau diambil pada sumber daya.

Contoh

```
"Action": {
    "ActionType": "PORT_PROBE",
    "PortProbeAction": {
        "PortProbeDetails": [
            {
                "LocalPortDetails": {
                    "Port": 80,
                    "PortName": "HTTP"
```

```
                  },
                "LocalIpDetails": {
                     "IpAddressV4": "192.0.2.0"
                 },
                "RemoteIpDetails": {
                    "Country": {
                        "CountryName": "Example Country"
                    },
                    "City": {
                        "CityName": "Example City"
                    },
                   "GeoLocation": {
                       "Lon": 0,
                       "Lat": 0
                   },
                   "Organization": {
                       "AsnOrg": "ExampleASO",
                       "Org": "ExampleOrg",
                       "Isp": "ExampleISP",
                       "Asn": 64496
                   }
                }
            }
        ],
        "Blocked": false
    }
}
```

AwsAccountName

Akun AWS Nama yang digunakan temuan itu.

Contoh

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Nama perusahaan untuk produk yang menghasilkan temuan. Untuk temuan berbasis kontrol, perusahaan adalah. AWS

Security Hub CSPM mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan `BatchImportFindings` atau `BatchUpdateFindings`.

Pengecualian untuk ini adalah ketika Anda menggunakan integrasi kustom. Lihat the section called “Integrasi produk kustom”.

Saat Anda menggunakan konsol CSPM Security Hub untuk memfilter temuan berdasarkan nama perusahaan, Anda menggunakan atribut ini. Saat Anda menggunakan Security Hub CSPM API untuk memfilter temuan berdasarkan nama perusahaan, Anda menggunakan `aws/securityhub/CompanyName` atribut di bawah. `ProductFields` Security Hub CSPM tidak menyinkronkan kedua atribut tersebut.

Contoh

```
"CompanyName": "AWS"
```

Kepatuhan

Ob `Compliance` jek biasanya memberikan rincian tentang temuan kontrol, seperti standar yang berlaku dan status pemeriksaan kontrol.

Contoh

```
"Compliance": {
    "AssociatedStandards": [
        {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
        {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
        {"StandardsId": "standards/nist-800-53/v/5.0.0"}
    ],
    "RelatedRequirements": [
        "NIST.800-53.r5 AC-4",
        "NIST.800-53.r5 AC-4(21)",
        "NIST.800-53.r5 SC-7",
        "NIST.800-53.r5 SC-7(11)",
        "NIST.800-53.r5 SC-7(16)",
        "NIST.800-53.r5 SC-7(21)",
        "NIST.800-53.r5 SC-7(4)",
        "NIST.800-53.r5 SC-7(5)"
    ],
    "SecurityControlId": "EC2.18",
    "SecurityControlParameters":[
        {
            "Name": "authorizedTcpPorts",
            "Value": ["80", "443"]
        },
```

```
        {
            "Name": "authorizedUdpPorts",
            "Value": ["427"]
        }
    ],
    "Status": "NOT_AVAILABLE",
    "StatusReasons": [
        {
            "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
            "Description": "This finding has a compliance status of NOT AVAILABLE
 because AWS Config sent Security Hub CSPM a finding with a compliance state of Not
 Applicable. The potential reasons for a Not Applicable finding from Config are that
 (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has
 been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule
 itself includes scenarios where Not Applicable is returned. The specific reason why
 Not Applicable is returned is not available in the Config rule evaluation."
        }
    ]
}
```

Kepercayaan

Kemungkinan bahwa temuan secara akurat mengidentifikasi perilaku atau masalah yang dimaksudkan untuk diidentifikasi.

`Confidence`seharusnya hanya diperbarui menggunakan `BatchUpdateFindings`.

Menemukan penyedia yang ingin memberikan nilai untuk `Confidence` harus menggunakan `Confidence` atribut di bawah`FindingProviderFields`. Lihat the section called “Memperbarui temuan dengan FindingProviderFields”.

`Confidence`dinilai berdasarkan 0-100 menggunakan skala rasio. 0 berarti kepercayaan 0 persen, dan 100 berarti kepercayaan 100 persen. Misalnya, deteksi eksfiltrasi data berdasarkan penyimpangan statistik lalu lintas jaringan memiliki kepercayaan rendah karena eksfiltrasi aktual belum diverifikasi.

Contoh

```
"Confidence": 42
```

Kekritisan

Tingkat kepentingan yang diberikan pada sumber daya yang terkait dengan temuan.

`Criticality`seharusnya hanya diperbarui dengan memanggil operasi `BatchUpdateFindings` API. Jangan memperbarui objek ini dengan `BatchImportFindings`.

Menemukan penyedia yang ingin memberikan nilai untuk `Criticality` harus menggunakan `Criticality` atribut di bawah`FindingProviderFields`. Lihat the section called “Memperbarui temuan dengan FindingProviderFields”.

`Criticality`dinilai berdasarkan 0-100, menggunakan skala rasio yang hanya mendukung bilangan bulat penuh. Skor 0 berarti bahwa sumber daya yang mendasarinya tidak memiliki kekritisan, dan skor 100 dicadangkan untuk sumber daya yang paling kritis.

Untuk setiap sumber daya, pertimbangkan hal berikut saat menetapkan: `Criticality`

- Apakah sumber daya yang terpengaruh berisi data sensitif (misalnya, bucket S3 dengan PII)?
- Apakah sumber daya yang terpengaruh memungkinkan musuh untuk memperdalam akses mereka atau memperluas kemampuan mereka untuk melakukan aktivitas berbahaya tambahan (misalnya, akun sysadmin yang dikompromikan)?
- Apakah sumber daya merupakan aset penting bisnis (misalnya, sistem bisnis utama yang jika dikompromikan dapat memiliki dampak pendapatan yang signifikan)?

Anda dapat menggunakan pedoman berikut:

- Sumber daya yang mendukung sistem kritis misi atau berisi data yang sangat sensitif dapat dinilai dalam kisaran 75-100.
- Sumber daya yang memberi daya pada sistem penting (tetapi bukan kritis) atau berisi data yang cukup penting dapat dinilai dalam kisaran 25-74.
- Sumber daya yang memberi daya pada sistem yang tidak penting atau berisi data tidak sensitif harus diberi skor dalam kisaran 0-24.

Contoh

```
"Criticality": 99
```

Deteksi

Ob `Detection` jek memberikan rincian tentang penemuan urutan serangan dari Amazon GuardDuty Extended Threat Detection. GuardDuty menghasilkan penemuan urutan serangan ketika beberapa

peristiwa sejajar dengan aktivitas yang berpotensi mencurigakan. Untuk menerima temuan urutan GuardDuty serangan di AWS Security Hub CSPM, Anda harus GuardDuty mengaktifkan di akun Anda. Untuk informasi selengkapnya, lihat Det GuardDuty eksi Ancaman Diperpanjang Amazon di Panduan GuardDuty Pengguna Amazon.

Contoh

```
"Detection": {
    "Sequence": {
     "Uid": "1111111111111-184ec3b9-cf8d-452d-9aad-f5bdb7afb010",
     "Actors": [{
      "Id": "USER:AROA987654321EXAMPLE:i-b188560f:1234567891",
      "Session": {
       "Uid": "1234567891",
       "MfAStatus": "DISABLED",
       "CreatedTime": "1716916944000",
       "Issuer": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      },
      "User": {
       "CredentialUid": "ASIAIOSFODNN7EXAMPLE",
       "Name": "ec2_instance_role_production",
       "Type": "AssumedRole",
       "Uid": "AROA987654321EXAMPLE:i-b188560f",
       "Account": {
        "Uid": "AccountId",
        "Name": "AccountName"
       }
      }
     }],
     "Endpoints": [{
      "Id": "EndpointId",
      "Ip": "203.0.113.1",
      "Domain": "example.com",
      "Port": 4040,
      "Location": {
       "City": "New York",
       "Country": "US",
       "Lat": 40.7123,
       "Lon": -74.0068
      },
      "AutonomousSystem": {
       "Name": "AnyCompany",
       "Number": 64496
```

```
      },
      "Connection": {
       "Direction": "INBOUND"
      }
     }],
     "Signals": [{
      "Id": "arn:aws:guardduty:us-east-1:123456789012:detector/
d0bfe135ab8b4dd8c3eaae7df9900073/finding/535a382b1bcc44d6b219517a29058fb7",
      "Title": "Someone ran a penetration test tool on your account.",
      "ActorIds": ["USER:AROA987654321EXAMPLE:i-b188560f:1234567891"],
      "Count": 19,
      "FirstSeenAt": 1716916943000,
      "SignalIndicators": [
       {
        "Key": "ATTACK_TACTIC",
        "Title": "Attack Tactic",
        "Values": [
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject"
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Data Destruction"
        ]
       },
      ],
      "LastSeenAt": 1716916944000,
      "Name": "Test:IAMUser/KaliLinux",
      "ResourceIds": [
       "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      ],
      "Type": "FINDING"
     }],
     "SequenceIndicators": [
      {
```

```
        "Key": "ATTACK_TACTIC",
        "Title": "Attack Tactic",
        "Values": [
         "Discovery",
         "Exfiltration",
         "Impact"
        ]
       },
       {
        "Key": "HIGH_RISK_API",
        "Title": "High Risk Api",
        "Values": [
         "s3:DeleteObject",
         "s3:GetObject",
         "s3:ListBuckets"
         "s3:ListObjects"
        ]
       },
       {
        "Key": "ATTACK_TECHNIQUE",
        "Title": "Attack Technique",
        "Values": [
         "Cloud Service Discovery",
         "Data Destruction"
        ]
       }
      ]
     }
}
```

FindingProviderFields

`FindingProviderFields`stermasuk atribut berikut:

- `Confidence`
- `Criticality`
- `RelatedFindings`
- `Severity`
- `Types`

Bidang sebelumnya bersarang di bawah `FindingProviderFields` objek, tetapi memiliki analog dengan nama yang sama dengan bidang ASFF tingkat atas. Ketika temuan baru dikirim ke Security Hub CSPM oleh penyedia pencari, Security Hub CSPM mengisi `FindingProviderFields` objek secara otomatis jika kosong berdasarkan bidang tingkat atas yang sesuai.

Menemukan penyedia dapat memperbarui `FindingProviderFields` dengan menggunakan pen `BatchImportFindings` goperasian Security Hub CSPM API. Penyedia pencarian tidak dapat memperbarui objek ini dengan `BatchUpdateFindings`.

Untuk detail tentang cara Security Hub CSPM menangani pembaruan dari `BatchImportFindings` ke `FindingProviderFields` dan ke atribut tingkat atas yang sesuai, lihat. the section called “Memperbarui temuan dengan FindingProviderFields”

Pelanggan dapat memperbarui bidang tingkat atas dengan menggunakan `BatchUpdateFindings` operasi. Pelanggan tidak dapat memperbarui`FindingProviderFields`.

Contoh

```
"FindingProviderFields": {
    "Confidence": 42,
    "Criticality": 99,
    "RelatedFindings":[
      {
        "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
        "Id": "123e4567-e89b-12d3-a456-426655440000"
      }
    ],
    "Severity": {
        "Label": "MEDIUM",
        "Original": "MEDIUM"
    },
    "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Menunjukkan kapan potensi masalah keamanan atau peristiwa yang ditangkap oleh temuan pertama kali diamati.

Stempel waktu ini menentukan kapan peristiwa atau kerentanan pertama kali diamati. Akibatnya, dapat berbeda dari stempel `CreatedAt` waktu, yang mencerminkan kapan catatan temuan ini dibuat.

Untuk temuan kontrol yang dihasilkan dan diperbarui Security Hub CSPM, stempel waktu ini juga dapat menunjukkan kapan status kepatuhan sumber daya baru-baru ini berubah. Untuk jenis temuan lain, stempel waktu ini harus tidak berubah di antara pembaruan catatan temuan, tetapi dapat diperbarui jika stempel waktu yang lebih akurat ditentukan.

Contoh

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Menunjukkan kapan potensi masalah keamanan atau peristiwa yang ditangkap oleh temuan baru-baru ini diamati oleh produk temuan keamanan.

Stempel waktu ini menentukan kapan peristiwa atau kerentanan terakhir atau terakhir diamati. Akibatnya, ini dapat berbeda dari stem `UpdatedAt` pel waktu, yang mencerminkan kapan catatan temuan ini terakhir atau terbaru diperbarui.

Anda dapat memberikan stempel waktu ini, tetapi tidak diperlukan pada pengamatan pertama. Jika Anda mengisi bidang ini pada pengamatan pertama, stempel waktu harus sama dengan stempel waktu. `FirstObservedAt` Anda harus memperbarui bidang ini untuk mencerminkan stempel waktu terakhir atau terakhir yang diamati setiap kali temuan diamati.

Contoh

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

Ob `Malware` jek menyediakan daftar malware yang terkait dengan temuan.

Contoh

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
```

```
]
```

Jaringan (Pensiunan)

Ob `Network` jek menyediakan informasi terkait jaringan tentang temuan.

Objek ini sudah pensiun. Untuk menyediakan data ini, Anda dapat memetakan data ke sumber daya di`Resources`, atau menggunakan `Action` objek.

Contoh

```
"Network": {
    "Direction": "IN",
    "OpenPortRange": {
        "Begin": 443,
        "End": 443
    },
    "Protocol": "TCP",
    "SourceIpV4": "1.2.3.4",
    "SourceIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "SourcePort": "42",
    "SourceDomain": "example1.com",
    "SourceMac": "00:0d:83:b1:c0:8e",
    "DestinationIpV4": "2.3.4.5",
    "DestinationIpV6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
    "DestinationPort": "80",
    "DestinationDomain": "example2.com"
}
```

NetworkPath

Ob `NetworkPath` jek memberikan informasi tentang jalur jaringan yang terkait dengan temuan. Setiap entri `NetworkPath` mewakili komponen jalur.

Contoh

```
"NetworkPath" : [
    {
        "ComponentId": "abc-01a234bc56d8901ee",
        "ComponentType": "AWS::EC2::InternetGateway",
        "Egress": {
            "Destination": {
                "Address": [ "192.0.2.0/24" ],
```

```
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": ["203.0.113.0/24"]
            }
        },
        "Ingress": {
            "Destination": {
                "Address": [ "198.51.100.0/24" ],
                "PortRanges": [
                    {
                        "Begin": 443,
                        "End": 443
                    }
                 ]
            },
            "Protocol": "TCP",
            "Source": {
                "Address": [ "203.0.113.0/24" ]
            }
        }
    }
]
```

Catatan

Ob `Note` jek menentukan catatan yang ditentukan pengguna yang dapat Anda tambahkan ke temuan.

Penyedia pencarian dapat memberikan catatan awal untuk temuan, tetapi tidak dapat menambahkan catatan setelah itu. Anda hanya dapat memperbarui catatan menggunakan `BatchUpdateFindings`.

Contoh

```
"Note": {
    "Text": "Don't forget to check under the mat.",
```

```
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

Ob `PatchSummary` jek memberikan ringkasan status kepatuhan patch untuk instance terhadap standar kepatuhan yang dipilih.

Contoh

```
"PatchSummary" : {
    "FailedCount" : 0,
    "Id" : "pb-123456789098",
    "InstalledCount" : 100,
    "InstalledOtherCount" : 1023,
    "InstalledPendingReboot" : 0,
    "InstalledRejectedCount" : 0,
    "MissingCount" : 100,
    "Operation" : "Install",
    "OperationEndTime" : "2018-09-27T23:39:31Z",
    "OperationStartTime" : "2018-09-27T23:37:31Z",
    "RebootOption" : "RebootIfNeeded"
}
```

Proses

Ob `Process` jek memberikan detail terkait proses tentang temuan.

Contoh:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Menunjukkan kapan Security Hub CSPM menerima temuan dan mulai memprosesnya.

Ini berbeda dari `CreatedAt` dan`UpdatedAt`, yang merupakan cap waktu yang diperlukan yang berhubungan dengan interaksi penyedia pencarian dengan masalah keamanan dan temuan. S `ProcessedAt` tempel waktu menunjukkan kapan Security Hub CSPM mulai memproses temuan. Temuan muncul di akun pengguna setelah pemrosesan selesai.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Jenis data di mana produk temuan keamanan dapat menyertakan detail spesifik solusi tambahan yang bukan bagian dari Format Penemuan Keamanan yang AWS ditentukan.

Untuk temuan yang dihasilkan oleh kontrol CSPM Security Hub, `ProductFields` termasuk informasi tentang kontrol. Lihat the section called “Menghasilkan dan memperbarui temuan kontrol”.

Bidang ini tidak boleh berisi data berlebihan dan tidak boleh berisi data yang bertentangan dengan AWS bidang Format Penemuan Keamanan.

Awalan `aws/` "" mewakili namespace yang dicadangkan hanya untuk AWS produk dan layanan dan tidak boleh diserahkan dengan temuan dari integrasi pihak ketiga.

Meskipun tidak diperlukan, produk harus memformat nama bidang sebagai`company-id/product-id/field-name`, di mana `company-id` dan `product-id` cocok dengan yang disediakan dalam `ProductArn` temuan.

Bidang referensi `Archival` digunakan saat Security Hub CSPM mengarsipkan temuan yang ada. Misalnya, Security Hub CSPM mengarsipkan temuan yang ada saat Anda menonaktifkan kontrol atau standar dan saat Anda mengaktifkan atau menonaktifkan temuan kontrol konsolid asi.

Bidang ini juga dapat mencakup informasi tentang standar yang mencakup kontrol yang menghasilkan temuan.

Contoh

```
"ProductFields": {
    "API", "DeleteTrail",
    "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
 consolidated control findings has been turned on or off. This causes findings in the
 previous state to be archived when new findings are being generated.",
    "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
    "aws/inspector/AssessmentTargetName": "My prod env",
```

```
    "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
    "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
    "generico/secure-pro/Action.Type", "AWS_API_CALL",
    "generico/secure-pro/Count": "6",
    "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Menyediakan nama produk yang menghasilkan temuan. Untuk temuan berbasis kontrol, nama produknya adalah Security Hub CSPM.

Security Hub CSPM mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan `BatchImportFindings` atau `BatchUpdateFindings`. Pengecualian untuk ini adalah ketika Anda menggunakan integrasi kustom. Lihat the section called "Integrasi produk kustom".

Saat Anda menggunakan konsol CSPM Security Hub untuk memfilter temuan berdasarkan nama produk, Anda menggunakan atribut ini.

Saat Anda menggunakan Security Hub CSPM API untuk memfilter temuan berdasarkan nama produk, Anda menggunakan `aws/securityhub/ProductName` atribut di bawah. `ProductFields`

Security Hub CSPM tidak menyinkronkan kedua atribut tersebut.

RecordState

Menyediakan status catatan temuan.

Secara default, ketika awalnya dihasilkan oleh layanan, temuan dipertimbangkan`ACTIVE`.

`ARCHIVED`Negara menunjukkan bahwa temuan harus disembunyikan dari pandangan. Temuan yang diarsipkan tidak segera dihapus. Anda dapat mencari, meninjau, dan melaporkannya. Security Hub CSPM secara otomatis mengarsipkan temuan berbasis kontrol jika sumber daya terkait dihapus, sumber daya tidak ada, atau kontrol dinonaktifkan.

`RecordState`dimaksudkan untuk menemukan penyedia, dan dapat diperbarui hanya dengan menggunakan `BatchImportFindings` operasi. Anda tidak dapat memperbaruinya dengan menggunakan `BatchUpdateFindings` operasi.

Untuk melacak status penyelidikan Anda ke dalam temuan, gunakan al `Workflow` ih-alih`RecordState`.

Jika status rekaman berubah dari `ARCHIVED` ke`ACTIVE`, dan status alur kerja temuan adalah `NOTIFIED` atau`RESOLVED`, Security Hub CSPM secara otomatis mengubah status alur kerja menjadi. `NEW`

Contoh

```
"RecordState": "ACTIVE"
```

Region

Menentukan Wilayah AWS dari mana temuan itu dihasilkan.

Security Hub CSPM mengisi atribut ini secara otomatis untuk setiap temuan. Anda tidak dapat memperbaruinya menggunakan `BatchImportFindings` atau `BatchUpdateFindings`.

Contoh

```
"Region": "us-west-2"
```

RelatedFindings

Menyediakan daftar temuan yang terkait dengan temuan saat ini.

`RelatedFindings`seharusnya hanya diperbarui dengan operasi `BatchUpdateFindings` API. Anda tidak boleh memperbarui objek ini dengan `BatchImportFindings`.

Untuk `BatchImportFindings` permintaan, penyedia pencarian harus menggunakan `RelatedFindings` objek di bawah `FindingProviderFields`.

Untuk melihat deskripsi `RelatedFindings` atribut, lihat `RelatedFinding` di Referensi AWS Security Hub API.

Contoh

```
"RelatedFindings": [
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000" },
    { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "AcmeNerfHerder-111111111111-x189dx7824" }
]
```

RiskAssessment

Contoh

```
"RiskAssessment": {
    "Posture": {
        "FindingTotal": 4,
        "Indicators": [
            {
                "Type": "Reachability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/1234567890abcdef0",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-east-2:123456789012:finding/
abcdef01234567890",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
                ]
            },
            {
                "Type": "Vulnerability",
                "Findings": [
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345abcdef6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    },
                    {
                        "Id": "arn:aws:inspector2:us-
east-2:123456789012:finding/021345ghijkl6789",
                        "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/
inspector",
                        "Title": "Finding title"
                    }
```

```
                ]
            }
        ]
    }
}
```

Remediasi

Ob `Remediation` jek memberikan informasi tentang langkah-langkah remediasi yang direkomendasikan untuk mengatasi temuan tersebut.

Contoh

```
"Remediation": {
    "Recommendation": {
        "Text": "For instructions on how to fix this issue, see the AWS Security Hub
 CSPM documentation for EC2.2.",
        "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"
    }
}
```

Sampel

Menentukan apakah temuan tersebut merupakan temuan sampel.

```
"Sample": true
```

SourceUrl

Ob `SourceUrl` jek menyediakan URL yang menautkan ke halaman tentang temuan saat ini dalam produk pencarian.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

Ob `ThreatIntelIndicator` jek memberikan rincian intelijen ancaman yang terkait dengan temuan.

Contoh

```
"ThreatIntelIndicators": [
```

```
  {
    "Category": "BACKDOOR",
    "LastObservedAt": "2018-09-27T23:37:31Z",
    "Source": "Threat Intel Weekly",
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",
    "Type": "IPV4_ADDRESS",
    "Value": "8.8.8.8",
  }
]
```

Ancaman

Ob Threats jek memberikan rincian tentang ancaman yang terdeteksi oleh temuan.

Contoh

```
"Threats": [{
    "FilePaths": [{
        "FileName": "b.txt",
        "FilePath": "/tmp/b.txt",
        "Hash": "sha256",
        "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
    }],
    "ItemCount": 3,
    "Name": "Iot.linux.mirai.vwisi",
    "Severity": "HIGH"
}]
```

UserDefinedFields

Menyediakan daftar pasangan string nama-nilai yang terkait dengan temuan. Ini adalah bidang khusus yang ditentukan pengguna yang ditambahkan ke temuan. Bidang-bidang ini dapat dibuat secara otomatis melalui konfigurasi spesifik Anda.

Penyedia pencarian tidak boleh menggunakan bidang ini untuk data yang dihasilkan produk. Sebagai gantinya, penyedia pencari dapat menggunakan `ProductFields` bidang untuk data yang tidak dipetakan ke bidang Format AWS Penemuan Keamanan standar.

Bidang-bidang ini hanya dapat diperbarui menggunakan `BatchUpdateFindings`.

Contoh

```
"UserDefinedFields": {
```

```
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Memberikan kebenaran temuan. Produk temuan dapat memberikan nilai `UNKNOWN` untuk bidang ini. Produk temuan harus memberikan nilai untuk bidang ini jika ada analog yang bermakna dalam sistem produk temuan. Bidang ini biasanya diisi oleh penentuan atau tindakan pengguna setelah menyelidiki temuan.

Penyedia pencarian dapat memberikan nilai awal untuk atribut ini, tetapi tidak dapat memperbaruinya setelah itu. Anda hanya dapat memperbarui atribut ini dengan menggunakan `BatchUpdateFindings`.

```
"VerificationState": "Confirmed"
```

Kerentanan

Ob Vulnerabilities jek menyediakan daftar kerentanan yang terkait dengan temuan.

Contoh

```
"Vulnerabilities" : [
    {
        "CodeVulnerabilities": [{
            "Cwes": [
                "CWE-798",
                "CWE-799"
            ],
            "FilePath": {
                "EndLine": 421,
                "FileName": "package-lock.json",
                "FilePath": "package-lock.json",
                "StartLine": 420
            },
                "SourceArn":"arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
        }],
        "Cvss": [
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
```

```
                "Version": "V3"
            },
            {
                "BaseScore": 4.7,
                "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
                "Version": "V2"
            }
        ],
        "EpssScore": 0.015,
        "ExploitAvailable": "YES",
        "FixAvailable": "YES",
        "Id": "CVE-2020-12345",
        "LastKnownExploitAt": "2020-01-16T00:01:35Z",
        "ReferenceUrls":[
           "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",
            "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
        ],
        "RelatedVulnerabilities": ["CVE-2020-12345"],
        "Vendor": {
            "Name": "Alas",
            "Url":"https://alas.aws.amazon.com/ALAS-2020-1337.html",
            "VendorCreatedAt":"2020-01-16T00:01:43Z",
            "VendorSeverity":"Medium",
            "VendorUpdatedAt":"2020-01-16T00:01:43Z"
        },
        "VulnerablePackages": [
            {
                "Architecture": "x86_64",
                "Epoch": "1",
                "FilePath": "/tmp",
                "FixedInVersion": "0.14.0",
                "Name": "openssl",
                "PackageManager": "OS",
                "Release": "16.amzn2.0.3",
                "Remediation": "Update aws-crt to 0.14.0",
                "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
                "SourceLayerHash":
 "sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
                "Version": "1.0.2k"
            }
        ]
    }
]
```

Alur kerja

Ob `Workflow` jek tersebut memberikan informasi tentang status penyelidikan terhadap suatu temuan.

Bidang ini dimaksudkan untuk digunakan pelanggan dengan alat remediasi, orkestrasi, dan tiket. Ini tidak dimaksudkan untuk menemukan penyedia.

Anda hanya dapat memperbarui `Workflow` bidang dengan `BatchUpdateFindings`. Pelanggan juga dapat memperbaruinya dari konsol. Lihat the section called “Mengatur status alur kerja temuan”.

Contoh

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState (Pensiun)

Objek ini dihentikan dan telah digantikan oleh `Status` bidang `Workflow` objek.

Bidang ini menyediakan status alur kerja dari sebuah temuan. Produk temuan dapat memberikan nilai `NEW` untuk bidang ini. Produk temuan dapat memberikan nilai untuk bidang ini jika ada analog yang bermakna dalam sistem produk temuan.

Contoh

```
"WorkflowState": "NEW"
```

Sumber daya Objek ASFF

Dalam Format AWS Penemuan Keamanan (ASFF), `Resources` objek memberikan informasi tentang sumber daya yang terlibat dalam temuan. Ini berisi array hingga 32 objek sumber daya. Untuk menentukan bagaimana nama sumber daya diformat, lihatAWS Format Penemuan Keamanan (ASFF). Untuk contoh dari setiap objek sumber daya, pilih sumber daya dari daftar berikut.

Topik

- Atribut sumber daya dalam ASFF
- AwsAmazonMQ sumber daya dalam ASFF
- AwsApiGateway sumber daya dalam ASFF

- AwsAppSync sumber daya dalam ASFF
- AwsAthena sumber daya dalam ASFF
- AwsAutoScaling sumber daya dalam ASFF
- AwsBackup sumber daya dalam ASFF
- AwsCertificateManager sumber daya dalam ASFF
- AwsCloudFormation sumber daya dalam ASFF
- AwsCloudFront sumber daya dalam ASFF
- AwsCloudTrail sumber daya dalam ASFF
- AwsCloudWatch sumber daya dalam ASFF
- AwsCodeBuild sumber daya dalam ASFF
- AwsDms sumber daya dalam ASFF
- AwsDynamoDB sumber daya dalam ASFF
- AwsEc2 sumber daya dalam ASFF
- AwsEcr sumber daya dalam ASFF
- AwsEcs sumber daya dalam ASFF
- AwsEfs sumber daya dalam ASFF
- AwsEks sumber daya dalam ASFF
- AwsElasticBeanstalk sumber daya dalam ASFF
- AwsElasticSearch sumber daya dalam ASFF
- AwsElb sumber daya dalam ASFF
- AwsEventBridge sumber daya dalam ASFF
- AwsGuardDuty sumber daya dalam ASFF
- AwsIam sumber daya dalam ASFF
- AwsKinesis sumber daya dalam ASFF
- AwsKms sumber daya dalam ASFF
- AwsLambda
- AwsMsk sumber daya dalam ASFF
- AwsNetworkFirewall sumber daya dalam ASFF
- AwsOpenSearchService sumber daya dalam ASFF
- AwsRds sumber daya dalam ASFF

- AwsRedshift sumber daya dalam ASFF
- AwsRoute53 sumber daya dalam ASFF
- AWSS3 sumber daya dalam ASFF
- AwsSageMaker sumber daya dalam ASFF
- AwsSecretsManager sumber daya dalam ASFF
- AwsSns sumber daya dalam ASFF
- AwsSqs sumber daya dalam ASFF
- AwsSsm sumber daya dalam ASFF
- AwsStepFunctions sumber daya dalam ASFF
- AwsWaf sumber daya dalam ASFF
- AwsXray sumber daya dalam ASFF
- CodeRepository objek dalam ASFF
- Kontainer objek dalam ASFF
- Lainnya objek dalam ASFF

Atribut sumber daya dalam ASFF

Berikut adalah deskripsi dan contoh untuk `Resources` objek dalam AWS Security Finding Format (ASFF). Untuk informasi selengkapnya tentang bidang ini, lihatSumber daya.

ApplicationArn

Mengidentifikasi Nama Sumber Daya Amazon (ARN) dari aplikasi yang terlibat dalam temuan.

Contoh

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

ApplicationName

Mengidentifikasi nama aplikasi yang terlibat dalam temuan.

Contoh

```
"ApplicationName": "SampleApp"
```

DataClassification

Bid DataClassification ang ini menyediakan informasi tentang data sensitif yang terdeteksi pada sumber daya.

Contoh

```
"DataClassification": {
    "DetailedResultsLocation": "Path_to_Folder_Or_File",
    "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
            "Code": "COMPLETE",
            "Reason": "Unsupportedfield"
        },
       "SensitiveData": [
            {
                "Category": "PERSONAL_INFORMATION",
                "Detections": [
                    {
                        "Count": 34,
                        "Type": "GE_PERSONAL_ID",
                        "Occurrences": {
                            "LineRanges": [
                                {
                                    "Start": 1,
                                    "End": 10,
                                    "StartColumn": 20
                                }
                            ],
                            "Pages": [],
                            "Records": [],
                            "Cells": []
                        }
                    },
                    {
                        "Count": 59,
                        "Type": "EMAIL_ADDRESS",
                        "Occurrences": {
                            "Pages": [
                                {
                                    "PageNumber": 1,
```

```
                            "OffsetRange": {
                                "Start": 1,
                                "End": 100,
                                "StartColumn": 10
                             },
                            "LineRange": {
                                "Start": 1,
                                "End": 100,
                                "StartColumn": 10
                            }
                        }
                    ]
                }
            },
            {
                "Count": 2229,
                "Type": "URL",
                "Occurrences": {
                   "LineRanges": [
                       {
                           "Start": 1,
                           "End": 13
                       }
                   ]
               }
           },
           {
               "Count": 13826,
               "Type": "NameDetection",
               "Occurrences": {
                    "Records": [
                        {
                            "RecordIndex": 1,
                            "JsonPath": "$.ssn.value"
                        }
                    ]
                }
           },
           {
               "Count": 32,
               "Type": "AddressDetection"
           }
       ],
       "TotalCount": 32
```

```
            }
        ],
        "CustomDataIdentifiers": {
            "Detections": [
                {
                    "Arn": "1712be25e7c7f53c731fe464f1c869b8",
                    "Name": "1712be25e7c7f53c731fe464f1c869b8",
                    "Count": 2,
                }
            ],
            "TotalCount": 2
        }
    }
}
```

Rincian

Bid Details ang ini memberikan informasi tambahan tentang sumber daya tunggal menggunakan objek yang sesuai. Setiap sumber daya harus disediakan dalam objek sumber daya terpisah dalam `Resources` objek.

Perhatikan bahwa jika ukuran temuan melebihi maksimum 240 KB, maka `Details` objek dihapus dari temuan. Untuk temuan kontrol yang menggunakan AWS Config aturan, Anda dapat melihat detail sumber daya di AWS Config konsol.

Security Hub CSPM menyediakan serangkaian detail sumber daya yang tersedia untuk jenis sumber daya yang didukung. Rincian ini sesuai dengan nilai-nilai `Type` objek. Gunakan jenis yang disediakan bila memungkinkan.

Misalnya, jika sumber daya adalah bucket S3, setel sumber daya `Type` ke `AwsS3Bucket` dan berikan detail sumber daya di `AwsS3Bucket` objek.

Ob `Other` jek memungkinkan Anda untuk menyediakan bidang dan nilai kustom. Anda menggunakan `Other` objek dalam kasus berikut:

- Jenis sumber daya (nilai sumber dayaType) tidak memiliki objek detail yang sesuai. Untuk memberikan rincian sumber daya, Anda menggunakan `Other` objek.
- Objek untuk jenis sumber daya tidak menyertakan semua bidang yang ingin Anda isi. Dalam hal ini, gunakan objek detail untuk jenis sumber daya untuk mengisi bidang yang tersedia. Gunakan `Other` objek untuk mengisi bidang yang tidak ada dalam objek tipe spesifik.

- Jenis sumber daya bukan salah satu jenis yang disediakan. Dalam hal ini, atur `Resource.Type` ke`Other`, dan gunakan `Other` objek untuk mengisi detail.

Contoh

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
      "HttpProtocolIpv6": "enabled",
      "HttpPutResponseHopLimit": 1,
      "HttpTokens": "optional",
      "InstanceMetadataTags": "disabled"
    },
    "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
    ],
    "SubnetId": "PublicSubnet",
    "Type": "i3.xlarge",
    "VirtualizationType": "hvm",
    "VpcId": "TestVPCIpv6"
  },
  "AwsS3Bucket": {
    "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
    "OwnerName": "acmes3bucketowner"
  },
  "Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

Pengidentifikasi untuk jenis sumber daya yang diberikan.

Untuk AWS sumber daya yang diidentifikasi oleh Amazon Resource Names (ARN), ini adalah ARN.

Untuk AWS sumber daya yang kekurangan ARN, ini adalah pengidentifikasi seperti yang didefinisikan oleh AWS layanan yang membuat sumber daya.

Untuk non-sumber AWS daya, ini adalah pengidentifikasi unik yang terkait dengan sumber daya.

Contoh

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partition

Partisi tempat sumber daya berada. Partisi adalah sekelompok Wilayah AWS. Masing-masing Akun AWS dicakup ke satu partisi.

Partisi berikut didukung:

- `aws` – Wilayah AWS
- `aws-cn`— Wilayah China
- `aws-us-gov` – AWS GovCloud (US) Region

Contoh

```
"Partition": "aws"
```

Region

Kode untuk Wilayah AWS tempat sumber daya ini berada. Untuk daftar kode Wilayah, lihat Titik akhir regional.

Contoh

```
"Region": "us-west-2"
```

ResourceRole

Mengidentifikasi peran sumber daya dalam temuan. Sumber daya adalah target aktivitas pencarian atau aktor yang melakukan aktivitas tersebut.

Contoh

```
"ResourceRole": "target"
```

Tanda

Bidang ini menyediakan kunci tag dan informasi nilai untuk sumber daya yang terlibat dalam temuan. Anda dapat menandai sumber daya yang didukung oleh pen `GetResources` goperasian API Pen AWS Resource Groups andaan. Security Hub CSPM memanggil operasi ini melalui peran yang ditautkan layanan dan mengambil tag sumber daya jika `Resource.Id` bidang AWS Security Finding Format (ASFF) diisi dengan ARN sumber daya. AWS ID sumber daya yang tidak valid diabaikan.

Anda dapat menambahkan tag sumber daya ke temuan yang dicerna oleh Security Hub CSPM, termasuk temuan dari produk terintegrasi Layanan AWS dan pihak ketiga.

Menambahkan tag memberi tahu Anda tag yang terkait dengan sumber daya pada saat temuan diproses. Anda dapat menyertakan `Tags` atribut hanya untuk sumber daya yang memiliki tag terkait. Jika sumber daya tidak memiliki tag terkait, jangan sertakan `Tags` atribut dalam temuan.

Dimasukkannya tag sumber daya dalam temuan menghilangkan kebutuhan untuk membangun jalur pengayaan data atau memperkaya metadata temuan keamanan secara manual. Anda juga dapat menggunakan tag untuk mencari atau memfilter temuan dan wawasan serta membuat aturan otomatisasi.

Untuk informasi tentang batasan yang berlaku untuk tag, lihat Batas dan persyaratan penamaan tag.

Anda hanya dapat memberikan tag yang ada pada AWS sumber daya di bidang ini. Untuk menyediakan data yang tidak ditentukan dalam Format Pen AWS emuan Keamanan, gunakan subbidang `Other` detail.

Contoh

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Tipe

Jenis sumber daya yang Anda berikan rinciannya.

Bila memungkinkan, gunakan salah satu jenis sumber daya yang disediakan, seperti `AwsEc2Instance` atau`AwsS3Bucket`.

Jika jenis sumber daya tidak cocok dengan salah satu jenis sumber daya yang disediakan, setel sumber daya `Type` ke`Other`, dan gunakan subbidang `Other` detail untuk mengisi detail.

Nilai yang didukung tercantum di bawah Sumber Daya.

Contoh

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsAmazonMQ` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsAmazonMQBroker

`AwsAmazonMQBroker`memberikan informasi tentang broker Amazon MQ, yang merupakan lingkungan broker pesan yang berjalan di Amazon MQ.

Contoh berikut menunjukkan ASFF untuk `AwsAmazonMQBroker` objek. Untuk melihat deskripsi `AwsAmazonMQBroker` atribut, lihat AwsAmazonMQBroker di Referensi AWS Security Hub API.

Contoh

```
"AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": true,
    "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "BrokerName": "TestBroker",
    "Configuration": {
        "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "Revision": 1
    },
    "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
    "EncryptionOptions": {
        "UseAwsOwnedKey": true
    },
    "EngineType": "ActiveMQ",
```

```
    "EngineVersion": "5.17.2",
    "HostInstanceType": "mq.t2.micro",
    "Logs": {
        "Audit": false,
        "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
        "General": false,
        "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
    },
    "MaintenanceWindowStartTime": {
        "DayOfWeek": "MONDAY",
        "TimeOfDay": "22:00",
        "TimeZone": "UTC"
    },
    "PubliclyAccessible": true,
    "SecurityGroups": [
        "sg-021345abcdef6789"
    ],
    "StorageType": "efs",
    "SubnetIds": [
        "subnet-1234567890abcdef0",
        "subnet-abcdef01234567890"
    ],
    "Users": [
        {
            "Username": "admin"
        }
    ]
}
```

AwsApiGateway sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsApiGateway` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsApiGatewayRestApi

Ob `AwsApiGatewayRestApi` jek berisi informasi tentang REST API di versi 1 dari Amazon API Gateway.

Berikut ini adalah contoh `AwsApiGatewayRestApi` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayRestApi` atribut, lihat AwsApiGatewayRestApiDetails di Referensi AWS Security Hub API.

Contoh

```
AwsApiGatewayRestApi: {
    "Id": "exampleapi",
    "Name": "Security Hub",
    "Description": "AWS Security Hub",
    "CreatedDate": "2018-11-18T10:20:05-08:00",
    "Version": "2018-10-26",
    "BinaryMediaTypes" : ["-'*~1*'"],
    "MinimumCompressionSize": 1024,
    "ApiKeySource": "AWS_ACCOUNT_ID",
    "EndpointConfiguration": {
        "Types": [
            "REGIONAL"
        ]
    }
}
```

AwsApiGatewayStage

Ob `AwsApiGatewayStage` jek menyediakan informasi tentang tahap Amazon API Gateway versi 1.

Berikut ini adalah contoh `AwsApiGatewayStage` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayStage` atribut, lihat AwsApiGatewayStageDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayStage": {
    "DeploymentId": "n7hlmf",
    "ClientCertificateId": "a1b2c3",
    "StageName": "Prod",
    "Description" : "Stage Description",
    "CacheClusterEnabled": false,
    "CacheClusterSize" : "1.6",
    "CacheClusterStatus": "NOT_AVAILABLE",
    "MethodSettings": [
        {
            "MetricsEnabled": true,
```

```
            "LoggingLevel": "INFO",
            "DataTraceEnabled": false,
            "ThrottlingBurstLimit": 100,
            "ThrottlingRateLimit": 5.0,
            "CachingEnabled": false,
            "CacheTtlInSeconds": 300,
            "CacheDataEncrypted": false,
            "RequireAuthorizationForCacheControl": true,
            "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
            "HttpMethod": "POST",
            "ResourcePath": "/echo"
        }
    ],
    "Variables": {"test": "value"},
    "DocumentationVersion": "2.0",
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "CanarySettings": {
        "PercentTraffic": 0.0,
        "DeploymentId": "ul73s8",
        "StageVariableOverrides" : [
            "String" : "String"
        ],
        "UseStageCache": false
    },
    "TracingEnabled": false,
    "CreatedDate": "2018-07-11T10:55:18-07:00",
```

```
    "LastUpdatedDate": "2020-08-26T11:51:04-07:00",
    "WebAclArn" : "arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822"
}
```

AwsApiGatewayV2Api

Ob `AwsApiGatewayV2Api` jek berisi informasi tentang API versi 2 di Amazon API Gateway.

Berikut ini adalah contoh `AwsApiGatewayV2Api` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Api` atribut, lihat AwsApiGatewayV2ApiDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayV2Api": {
    "ApiEndpoint": "https://example.us-west-2.amazonaws.com",
    "ApiId": "a1b2c3d4",
    "ApiKeySelectionExpression": "$request.header.x-api-key",
    "CreatedDate": "2020-03-28T00:32:37Z",
   "Description": "ApiGatewayV2 Api",
   "Version": "string",
    "Name": "my-api",
    "ProtocolType": "HTTP",
    "RouteSelectionExpression": "$request.method $request.path",
   "CorsConfiguration": {
        "AllowOrigins": [ "*" ],
        "AllowCredentials": true,
        "ExposeHeaders": [ "string" ],
        "MaxAge": 3000,
        "AllowMethods": [
          "GET",
          "PUT",
          "POST",
          "DELETE",
          "HEAD"
        ],
        "AllowHeaders": [ "*" ]
    }
}
```

AwsApiGatewayV2Stage

`AwsApiGatewayV2Stage`berisi informasi tentang tahap versi 2 untuk Amazon API Gateway.

Berikut ini adalah contoh `AwsApiGatewayV2Stage` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsApiGatewayV2StageDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsApiGatewayV2Stage": {
    "CreatedDate": "2020-04-08T00:36:05Z",
    "Description" : "ApiGatewayV2",
    "DefaultRouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "DeploymentId": "x1zwyv",
    "LastUpdatedDate": "2020-04-08T00:36:13Z",
    "RouteSettings": {
        "DetailedMetricsEnabled": false,
        "LoggingLevel": "INFO",
        "DataTraceEnabled": true,
        "ThrottlingBurstLimit": 100,
        "ThrottlingRateLimit": 50
    },
    "StageName": "prod",
    "StageVariables": [
        "function": "my-prod-function"
    ],
    "AccessLogSettings": {
        "Format": "{\"requestId\": \"$context.requestId\", \"extendedRequestId
\": \"$context.extendedRequestId\", \"ownerAccountId\": \"$context.accountId\",
 \"requestAccountId\": \"$context.identity.accountId\", \"callerPrincipal\":
 \"$context.identity.caller\", \"httpMethod\": \"$context.httpMethod\", \"resourcePath
\": \"$context.resourcePath\", \"status\": \"$context.status\", \"requestTime
\": \"$context.requestTime\", \"responseLatencyMs\": \"$context.responseLatency
\", \"errorMessage\": \"$context.error.message\", \"errorResponseType\":
 \"$context.error.responseType\", \"apiId\": \"$context.apiId\", \"awsEndpointRequestId
\": \"$context.awsEndpointRequestId\", \"domainName\": \"$context.domainName\", \"stage
\": \"$context.stage\", \"xrayTraceId\": \"$context.xrayTraceId\", \"sourceIp\":
```

```
 \"$context.identity.sourceIp\", \"user\": \"$context.identity.user\", \"userAgent
\": \"$context.identity.userAgent\", \"userArn\": \"$context.identity.userArn\",
 \"integrationLatency\": \"$context.integrationLatency\", \"integrationStatus
\": \"$context.integrationStatus\", \"authorizerIntegrationLatency\":
 \"$context.authorizer.integrationLatency\" }",
        "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
    },
    "AutoDeploy": false,
    "LastDeploymentStatusMessage": "Message",
    "ApiGatewayManaged": true,
}
```

AwsAppSync sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsAppSync` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsAppSyncGraphQLApi

`AwsAppSyncGraphQLApi`memberikan informasi tentang AWS AppSync GraphQL API, yang merupakan konstruksi tingkat atas untuk aplikasi Anda.

Contoh berikut menunjukkan ASFF untuk `AwsAppSyncGraphQLApi` objek. Untuk melihat deskripsi `AwsAppSyncGraphQLApi` atribut, lihat AwsAppSyncGraphQLApi di Referensi AWS Security Hub API.

Contoh

```
"AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
    {
     "AuthenticationType": "AWS_LAMBDA",
     "LambdaAuthorizerConfig": {
      "AuthorizerResultTtlInSeconds": 300,
      "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
     }
    },
    {
```

```
     "AuthenticationType": "AWS_IAM"
    }
    ],
    "ApiId": "021345abcdef6789",
    "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
    "AuthenticationType": "API_KEY",
    "Id": "021345abcdef6789",
    "LogConfig": {
     "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-
graphqlapi-logs-eu-central-1",
     "ExcludeVerboseContent": true,
     "FieldLogLevel": "ALL"
    },
    "Name": "My AppSync App",
    "XrayEnabled": true,
}
```

AwsAthena sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsAthena` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsAthenaWorkGroup

`AwsAthenaWorkGroup`memberikan informasi tentang kelompok kerja Amazon Athena. Workgroup membantu Anda memisahkan pengguna, tim, aplikasi, atau beban kerja. Ini juga membantu Anda menetapkan batasan pemrosesan data dan melacak biaya.

Contoh berikut menunjukkan ASFF untuk `AwsAthenaWorkGroup` objek. Untuk melihat deskripsi `AwsAthenaWorkGroup` atribut, lihat AwsAthenaWorkGroup di Referensi AWS Security Hub API.

Contoh

```
"AwsAthenaWorkGroup": {
    "Description": "My workgroup for prod workloads",
    "Name": "MyWorkgroup",
    "WorkgroupConfiguration" {
        "ResultConfiguration": {
            "EncryptionConfiguration": {
                "EncryptionOption": "SSE_KMS",
```

```
                "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
            }
        }
    },
        "State": "ENABLED"
}
```

AwsAutoScaling sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsAutoScaling` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsAutoScalingAutoScalingGroup

Ob `AwsAutoScalingAutoScalingGroup` jek memberikan rincian tentang grup penskalaan otomatis.

Berikut ini adalah contoh `AwsAutoScalingAutoScalingGroup` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsAutoScalingAutoScalingGroup` atribut, lihat AwsAutoScalingAutoScalingGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsAutoScalingAutoScalingGroup": {
        "CreatedTime": "2017-10-17T14:47:11Z",
        "HealthCheckGracePeriod": 300,
        "HealthCheckType": "EC2",
        "LaunchConfigurationName": "mylaunchconf",
        "LoadBalancerNames": [],
        "LaunchTemplate": {
            "LaunchTemplateId": "string",
            "LaunchTemplateName": "string",
            "Version": "string"
        },
        "MixedInstancesPolicy": {
            "InstancesDistribution": {
                "OnDemandAllocationStrategy": "prioritized",
                "OnDemandBaseCapacity": number,
```

```
                "OnDemandPercentageAboveBaseCapacity": number,
                "SpotAllocationStrategy": "lowest-price",
                "SpotInstancePools": number,
                "SpotMaxPrice": "string"
            },
            "LaunchTemplate": {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "string",
                    "LaunchTemplateName": "string",
                    "Version": "string"
                 },
                "CapacityRebalance": true,
                "Overrides": [
                    {
                       "InstanceType": "string",
                       "WeightedCapacity": "string"
                    }
                ]
            }
        }
    }
}
```

AwsAutoScalingLaunchConfiguration

Ob `AwsAutoScalingLaunchConfiguration` jek memberikan rincian tentang konfigurasi peluncuran.

Berikut ini adalah contoh `AwsAutoScalingLaunchConfiguration` penemuan dalam AWS Security Finding Format (ASFF).

Untuk melihat deskripsi `AwsAutoScalingLaunchConfiguration` atribut, lihat AwsAutoScalingLaunchConfigurationDetails di Referensi AWS Security Hub API.

Contoh

```
AwsAutoScalingLaunchConfiguration: {
    "LaunchConfigurationName": "newtest",
    "ImageId": "ami-058a3739b02263842",
    "KeyName": "55hundredinstance",
    "SecurityGroups": [ "sg-01fce87ad6e019725" ],
    "ClassicLinkVpcSecurityGroups": [],
    "UserData": "...Base64-Encoded user data..."
```

```
    "InstanceType": "a1.metal",
    "KernelId": "",
    "RamdiskId": "ari-a51cf9cc",
    "BlockDeviceMappings": [
        {
            "DeviceName": "/dev/sdh",
            "Ebs": {
                "VolumeSize": 30,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true,
                "SnapshotId": "snap-ffaa1e69",
                "VirtualName": "ephemeral1"
            }
        },
        {
            "DeviceName": "/dev/sdb",
            "NoDevice": true
        },
        {
            "DeviceName": "/dev/sda1",
            "Ebs": {
                "SnapshotId": "snap-02420cd3d2dea1bc0",
                "VolumeSize": 8,
                "VolumeType": "gp2",
                "DeleteOnTermination": true,
                "Encrypted": false
            }
        },
        {
            "DeviceName": "/dev/sdi",
            "Ebs": {
                "VolumeSize": 20,
                "VolumeType": "gp2",
                "DeleteOnTermination": false,
                "Encrypted": true
            }
        },
        {
            "DeviceName": "/dev/sdc",
            "NoDevice": true
        }
    ],
    "InstanceMonitoring": {
```

```
        "Enabled": false
    },
    "CreatedTime": 1620842933453,
    "EbsOptimized": false,
    "AssociatePublicIpAddress": true,
    "SpotPrice": "0.045"
}
```

AwsBackup sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsBackup` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsBackupBackupPlan

Ob `AwsBackupBackupPlan` jek memberikan informasi tentang rencana AWS Backup cadangan. R AWS Backup encana cadangan adalah ekspresi kebijakan yang menentukan kapan dan bagaimana Anda ingin membuat cadangan AWS sumber daya Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsBackupBackupPlan` objek. Untuk melihat deskripsi `AwsBackupBackupPlan` atribut, lihat AwsBackupBackupPlan di Referensi AWS Security Hub API.

Contoh

```
"AwsBackupBackupPlan": {
    "BackupPlan": {
     "AdvancedBackupSettings": [{
      "BackupOptions": {
       "WindowsVSS":"enabled"
      },
      "ResourceType":"EC2"
     }],
     "BackupPlanName": "test",
     "BackupPlanRule": [{
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
```

```
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "DailyBackups",
      "ScheduleExpression": "cron(0 5 ? * * *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
      },
      {
      "CompletionWindowMinutes": 10080,
      "CopyActions": [{
       "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
       "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
       }
      }],
      "Lifecycle": {
       "DeleteAfterDays": 35
      },
      "RuleName": "Monthly",
      "ScheduleExpression": "cron(0 5 1 * ? *)",
      "StartWindowMinutes": 480,
      "TargetBackupVault": "Default"
     }]
    },
    "BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
    "VersionId": "ZDVjNDIzMjItYTZiNS00NzczLTg4YzctNmExMWM2NjZhY2E1"
}
```

AwsBackupBackupVault

Ob `AwsBackupBackupVault` jek memberikan informasi tentang bran AWS Backup kas cadangan. Vault AWS Backup cadangan adalah wadah yang menyimpan dan mengatur cadangan Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsBackupBackupVault` objek. Untuk melihat deskripsi `AwsBackupBackupVault` atribut, lihat AwsBackupBackupVault di Referensi AWS Security Hub API.

Contoh

```
"AwsBackupBackupVault": {
    "AccessPolicy": {
     "Statement": [{
      "Action": [
       "backup:DeleteBackupVault",
       "backup:DeleteBackupVaultAccessPolicy",
       "backup:DeleteRecoveryPoint",
       "backup:StartCopyJob",
       "backup:StartRestoreJob",
       "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
       "AWS": "*"
      },
      "Resource": "*"
     }],
     "Version": "2012-10-17"
    },
    "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/
automatic-backup-vault",
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "EncrytionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "Notifications": {
     "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED",
 "COPY_JOB_STARTED"],
     "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
    }
}
```

AwsBackupRecoveryPoint

Ob `AwsBackupRecoveryPoint` jek memberikan informasi tentang AWS Backup cadangan, juga disebut sebagai titik pemulihan. Titik AWS Backup pemulihan mewakili konten sumber daya pada waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsBackupRecoveryPoint` objek. Untuk melihat deskripsi `AwsBackupBackupVault` atribut, lihat AwsBackupRecoveryPoint di Referensi AWS Security Hub API.

Contoh

```
"AwsBackupRecoveryPoint": {
    "BackupSizeInBytes": 0,
    "BackupVaultName": "aws/efs/automatic-backup-vault",
    "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/
automatic-backup-vault",
    "CalculatedLifecycle": {
     "DeleteAt": "2021-08-30T06:51:58.271Z",
     "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
    },
    "CompletionDate": "2021-07-26T07:21:40.361Z",
    "CreatedBy": {
     "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/
efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
     "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
     "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
    },
    "CreationDate": "2021-07-26T06:51:58.271Z",
    "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-
ba38-838bf8d06ca0",
    "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/
backup.amazonaws.com/AWSServiceRoleForBackup",
    "IsEncrypted": true,
    "LastRestoreTime": "2021-07-26T06:51:58.271Z",
    "Lifecycle": {
     "DeleteAfterDays": 35,
     "MoveToColdStorageAfterDays": 15
    },
    "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-
f1d5-4587-a7fd-0774c6e91268",
    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
```

```
    "StorageClass": "WARM"
}
```

AwsCertificateManager sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCertificateManager` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsCertificateManagerCertificate

Ob `AwsCertificateManagerCertificate` jek memberikan rincian tentang sertifikat AWS Certificate Manager (ACM).

Berikut ini adalah contoh `AwsCertificateManagerCertificate` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCertificateManagerCertificate` atribut, lihat AwsCertificateManagerCertificateDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
    "CreatedAt": "2019-05-24T18:12:02.000Z",
    "DomainName": "example.amazondomains.com",
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws."
             },
             "ValidationDomain": "example.amazondomains.com",
             "ValidationEmails": [sample_email@sample.com],
             "ValidationMethod": "DNS",
             "ValidationStatus": "SUCCESS"
        }
    ],
    "ExtendedKeyUsages": [
        {
```

```
            "Name": "TLS_WEB_SERVER_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.1"
        },
        {
            "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
            "OId": "1.3.6.1.5.5.7.3.2"
        }
    ],
    "FailureReason": "",
    "ImportedAt": "2018-08-17T00:13:00.000Z",
    "InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
    "IssuedAt": "2020-04-26T00:41:17.000Z",
    "Issuer": "Amazon",
    "KeyAlgorithm": "RSA-1024",
    "KeyUsages": [
        {
            "Name": "DIGITAL_SIGNATURE",
        },
        {
            "Name": "KEY_ENCIPHERMENT",
        }
    ],
    "NotAfter": "2021-05-26T12:00:00.000Z",
    "NotBefore": "2020-04-26T00:00:00.000Z",
    "Options": {
        "CertificateTransparencyLoggingPreference": "ENABLED",
    }
    "RenewalEligibility": "ELIGIBLE",
    "RenewalSummary": {
        "DomainValidationOptions": [
            {
                "DomainName": "example.amazondomains.com",
                "ResourceRecord": {
                    "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                    "Type": "CNAME",
                    "Value": "_example.acm-validations.aws.com",
                },
                "ValidationDomain": "example.amazondomains.com",
                "ValidationEmails": ["sample_email@sample.com"],
                "ValidationMethod": "DNS",
                "ValidationStatus": "SUCCESS"
            }
        ],
```

```
        "RenewalStatus": "SUCCESS",
        "RenewalStatusReason": "",
        "UpdatedAt": "2020-04-26T00:41:35.000Z",
    },
    "Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
    "SignatureAlgorithm": "SHA256WITHRSA",
    "Status": "ISSUED",
    "Subject": "CN=example.amazondomains.com",
    "SubjectAlternativeNames": ["example.amazondomains.com"],
    "Type": "AMAZON_ISSUED"
}
```

AwsCloudFormation sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCloudFormation` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsCloudFormationStack

Ob `AwsCloudFormationStack` jek memberikan rincian tentang AWS CloudFormation tumpukan yang bersarang sebagai sumber daya dalam template tingkat atas.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsCloudFormationStack` objek. Untuk melihat deskripsi `AwsCloudFormationStack` atribut, lihat AwsCloudFormationStackDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsCloudFormationStack": {
 "Capabilities": [
  "CAPABILITY_IAM",
  "CAPABILITY_NAMED_IAM"
 ],
 "CreationTime": "2022-02-18T15:31:53.161Z",
 "Description": "AWS CloudFormation Sample",
 "DisableRollback": true,
 "DriftInformation": {
  "StackDriftStatus": "DRIFTED"
 },
 "EnableTerminationProtection": false,
```

```
 "LastUpdatedTime": "2022-02-18T15:31:53.161Z",
 "NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
 ],
 "Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
 }],
 "RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
 "StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
 "StackName": "sample-stack",
 "StackStatus": "CREATE_COMPLETE",
 "StackStatusReason": "Success",
 "TimeoutInMinutes": 1
}
```


AwsCloudFront sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCloudFront` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsCloudFrontDistribution

Ob `AwsCloudFrontDistribution` jek memberikan rincian tentang konfigurasi CloudFront distribusi Amazon.

Berikut ini adalah contoh `AwsCloudFrontDistribution` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCloudFrontDistribution` atribut, lihat AwsCloudFrontDistributionDetails di Referensi AWS Security Hub API.

Contoh


```
"AwsCloudFrontDistribution": {
    "CacheBehaviors": {
        "Items": [
            {
               "ViewerProtocolPolicy": "https-only"
            }
```

```
        ]
    },
    "DefaultCacheBehavior": {
        "ViewerProtocolPolicy": "https-only"
    },
    "DefaultRootObject": "index.html",
    "DomainName": "d2wkuj2w9l34gt.cloudfront.net",
    "Etag": "E37HOT42DHPVYH",
    "LastModifiedTime": "2015-08-31T21:11:29.093Z",
    "Logging": {
        "Bucket": "myawslogbucket.s3.amazonaws.com",
        "Enabled": false,
        "IncludeCookies": false,
        "Prefix": "myawslog/"
    },
    "OriginGroups": {
         "Items": [
             {
                "FailoverCriteria": {
                    "StatusCodes": {
                        "Items": [
                            200,
                            301,
                            404
                        ]
                        "Quantity": 3
                    }
                }
             }
          ]
    },
    "Origins": {
          "Items": [
              {
                 "CustomOriginConfig": {
                     "HttpPort": 80,
                     "HttpsPort": 443,
                     "OriginKeepaliveTimeout": 60,
                     "OriginProtocolPolicy": "match-viewer",
                     "OriginReadTimeout": 30,
                     "OriginSslProtocols": {
                       "Items": ["SSLv3", "TLSv1"],
                       "Quantity": 2
                     }
```

```
                    }
                },
            ]
        },
                "DomainName": "amzn-s3-demo-bucket.s3.amazonaws.com",
                "Id": "my-origin",
                "OriginPath": "/production",
                "S3OriginConfig": {
                    "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
                }
            ]
        },
        "Status": "Deployed",
        "ViewerCertificate": {
               "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
               "Certificate": "ASCAJRRE5XYF52TKRY5M4",
               "CertificateSource": "iam",
               "CloudFrontDefaultCertificate": true,
               "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
               "MinimumProtocolVersion": "TLSv1.2_2021",
               "SslSupportMethod": "sni-only"
         },
         "WebAclId": "waf-1234567890"
}
```

AwsCloudTrail sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCloudTrail` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsCloudTrailTrail

Ob `AwsCloudTrailTrail` jek memberikan detail tentang AWS CloudTrail jejak.

Berikut ini adalah contoh `AwsCloudTrailTrail` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCloudTrailTrail` atribut, lihat AwsCloudTrailTrailDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsCloudTrailTrail": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",
    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}
```

AwsCloudWatch sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCloudWatch` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsCloudWatchAlarm

Ob `AwsCloudWatchAlarm` jek memberikan detail tentang CloudWatch alarm Amazon yang menonton metrik atau melakukan tindakan saat alarm berubah status.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsCloudWatchAlarm` objek. Untuk melihat deskripsi `AwsCloudWatchAlarm` atribut, lihat AwsCloudWatchAlarmDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsCloudWatchAlarm": {
 "ActionsEnabled": true,
 "AlarmActions": [
```

```
  "arn:aws:automate:region:ec2:stop",
  "arn:aws:automate:region:ec2:terminate"
 ],
 "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
 "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
 "AlarmDescription": "Alarm Example",
 "AlarmName": "Example",
 "ComparisonOperator": "GreaterThanOrEqualToThreshold",
 "DatapointsToAlarm": 1,
 "Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
 }],
 "EvaluateLowSampleCountPercentile": "evaluate",
 "EvaluationPeriods": 1,
 "ExtendedStatistic": "p99.9",
 "InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
 ],
 "MetricName": "Sample Metric",
 "Namespace": "YourNamespace",
 "OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
 ],
 "Period": 1,
 "Statistic": "SampleCount",
 "Threshold": 12.3,
 "ThresholdMetricId": "t1",
 "TreatMissingData": "notBreaching",
 "Unit": "Kilobytes/Second"
}
```

AwsCodeBuild sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsCodeBuild` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsCodeBuildProject

Ob `AwsCodeBuildProject` jek memberikan informasi tentang sebuah AWS CodeBuild proyek.

Berikut ini adalah contoh `AwsCodeBuildProject` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsCodeBuildProject` atribut, lihat AwsCodeBuildProjectDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsCodeBuildProject": {
   "Artifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "SecondaryArtifacts": [
      {
          "ArtifactIdentifier": "string",
          "EncryptionDisabled": boolean,
          "Location": "string",
          "Name": "string",
          "NamespaceType": "string",
          "OverrideArtifactName": boolean,
          "Packaging": "string",
          "Path": "string",
          "Type": "string"
       }
   ],
   "EncryptionKey": "string",
   "Certificate": "string",
   "Environment": {
      "Certificate": "string",
      "EnvironmentVariables": [
           {
                "Name": "string",
                "Type": "string",
                "Value": "string"
           }
```

```
      ],
   "ImagePullCredentialsType": "string",
   "PrivilegedMode": boolean,
   "RegistryCredential": {
       "Credential": "string",
       "CredentialProvider": "string"
   },
   "Type": "string"
   },
   "LogsConfig": {
        "CloudWatchLogs": {
             "GroupName": "string",
             "Status": "string",
             "StreamName": "string"
        },
        "S3Logs": {
             "EncryptionDisabled": boolean,
             "Location": "string",
             "Status": "string"
        }
   },
   "Name": "string",
   "ServiceRole": "string",
   "Source": {
        "Type": "string",
        "Location": "string",
        "GitCloneDepth": integer
   },
   "VpcConfig": {
        "VpcId": "string",
        "Subnets": ["string"],
        "SecurityGroupIds": ["string"]
   }
}
```

AwsDms sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsDms` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsDmsEndpoint

Ob `AwsDmsEndpoint` jek memberikan informasi tentang titik akhir AWS Database Migration Service (AWS DMS). Titik akhir menyediakan koneksi, jenis penyimpanan data, dan informasi lokasi tentang penyimpanan data Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsEndpoint` objek. Untuk melihat deskripsi `AwsDmsEndpoint` atribut, lihat AwsDmsEndpointDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWFI",
    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVFVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}
```

AwsDmsReplicationInstance

Ob `AwsDmsReplicationInstance` jek memberikan informasi tentang instance replikasi AWS Database Migration Service (AWS DMS). DMS menggunakan instance replikasi untuk terhubung ke penyimpanan data sumber Anda, membaca data sumber, dan memformat data untuk dikonsumsi oleh penyimpanan data target.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsReplicationInstance` objek. Untuk melihat deskripsi `AwsDmsReplicationInstance` atribut, lihat AwsDmsReplicationInstanceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsDmsReplicationInstance": {
    "AllocatedStorage": 50,
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1b",
    "EngineVersion": "3.5.1",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
    "MultiAZ": false,
    "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
    "PubliclyAccessible": true,
    "ReplicationInstanceClass": "dms.c5.xlarge",
    "ReplicationInstanceIdentifier": "second-replication-instance",
    "ReplicationSubnetGroup": {
        "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
    },
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-003a34e205138138b"
        }
    ]
}
```

AwsDmsReplicationTask

Ob `AwsDmsReplicationTask` jek memberikan informasi tentang tugas replikasi AWS Database Migration Service (AWS DMS). Tugas replikasi memindahkan sekumpulan data dari titik akhir sumber ke titik akhir target.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsDmsReplicationInstance` objek. Untuk melihat deskripsi `AwsDmsReplicationInstance` atribut, lihat AwsDmsReplicationInstance di Referensi AWS Security Hub API.

Contoh

```
"AwsDmsReplicationTask": {
    "CdcStartPosition": "2023-08-28T14:26:22",
    "Id": "arn:aws:dms:us-
east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
    "MigrationType": "cdc",
    "ReplicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4YOUGIMYJUI",
    "ReplicationTaskIdentifier": "test-task",
```

```
    "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
\"EnableLogContext\":false,\"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"TRANSFORMATION\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",
\"Id\":\"SOURCE_UNLOAD\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"IO\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TARGET_LOAD\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"PERFORMANCE\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SOURCE_CAPTURE\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"SORTER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"REST_SERVER\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id
\":\"VALIDATOR_EXT\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":
\"TARGET_APPLY\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TASK_MANAGER
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"TABLES_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"METADATA_MANAGER\"},
{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_FACTORY\"},{\"Severity\":
\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMON\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT
\",\"Id\":\"ADDONS\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"DATA_STRUCTURE
\"},{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"COMMUNICATION\"},{\"Severity
\":\"LOGGER_SEVERITY_DEFAULT\",\"Id\":\"FILE_TRANSFER\"}],\"CloudWatchLogGroup
\":null,\"CloudWatchLogStream\":null},\"StreamBufferSettings\":{\"StreamBufferCount
\":3,\"CtrlStreamBufferSizeInMB\":5,\"StreamBufferSizeInMB\":8},\"ErrorBehavior
\":{\"FailOnNoTablesCaptured\":true,\"ApplyErrorUpdatePolicy\":\"LOG_ERROR\",
\"FailOnTransactionConsistencyBreached\":false,\"RecoverableErrorThrottlingMax\":1800,
\"DataErrorEscalationPolicy\":\"SUSPEND_TABLE\",\"ApplyErrorEscalationCount\":0,
\"RecoverableErrorStopRetryAfterThrottlingMax\":true,\"RecoverableErrorThrottling
\":true,\"ApplyErrorFailOnTruncationDdl\":false,\"DataTruncationErrorPolicy\":
\"LOG_ERROR\",\"ApplyErrorInsertPolicy\":\"LOG_ERROR\",\"EventErrorPolicy\":
\"IGNORE\",\"ApplyErrorEscalationPolicy\":\"LOG_ERROR\",\"RecoverableErrorCount
\":-1,\"DataErrorEscalationCount\":0,\"TableErrorEscalationPolicy\":\"STOP_TASK
\",\"RecoverableErrorInterval\":5,\"ApplyErrorDeletePolicy\":\"IGNORE_RECORD\",
\"TableErrorEscalationCount\":0,\"FullLoadIgnoreConflicts\":true,\"DataErrorPolicy
\":\"LOG_ERROR\",\"TableErrorPolicy\":\"SUSPEND_TABLE\"},\"TTSettings
\":{\"TTS3Settings\":null,\"TTRecordSettings\":null,\"EnableTT\":false},
\"FullLoadSettings\":{\"CommitRate\":10000,\"StopTaskCachedChangesApplied
\":false,\"StopTaskCachedChangesNotApplied\":false,\"MaxFullLoadSubTasks
\":8,\"TransactionConsistencyTimeout\":600,\"CreatePkAfterFullLoad\":false,
\"TargetTablePrepMode\":\"DO_NOTHING\"},\"TargetMetadata\":{\"ParallelApplyBufferSize
\":0,\"ParallelApplyQueuesPerThread\":0,\"ParallelApplyThreads\":0,\"TargetSchema
\":\"\",\"InlineLobMaxSize\":0,\"ParallelLoadQueuesPerThread\":0,\"SupportLobs
\":true,\"LobChunkSize\":64,\"TaskRecoveryTableEnabled\":false,\"ParallelLoadThreads
\":0,\"LobMaxSize\":0,\"BatchApplyEnabled\":false,\"FullLobMode\":true,
\"LimitedSizeLobMode\":false,\"LoadMaxFileSize\":0,\"ParallelLoadBufferSize\":0},
\"BeforeImageSettings\":null,\"ControlTablesSettings\":{\"historyTimeslotInMinutes
\":5,\"HistoryTimeslotInMinutes\":5,\"StatusTableEnabled\":false,
\"SuspendedTablesTableEnabled\":false,\"HistoryTableEnabled\":false,\"ControlSchema
```

```
\":\"\",\"FullLoadExceptionTableEnabled\":false},\"LoopbackPreventionSettings
\":null,\"CharacterSetSettings\":null,\"FailTaskWhenCleanTaskResourceFailed
\":false,\"ChangeProcessingTuning\":{\"StatementCacheSize\":50,\"CommitTimeout
\":1,\"BatchApplyPreserveTransaction\":true,\"BatchApplyTimeoutMin\":1,
\"BatchSplitSize\":0,\"BatchApplyTimeoutMax\":30,\"MinTransactionSize\":1000,
\"MemoryKeepTime\":60,\"BatchApplyMemoryLimit\":500,\"MemoryLimitTotal\":1024},
\"ChangeProcessingDdlHandlingPolicy\":{\"HandleSourceTableDropped\":true,
\"HandleSourceTableTruncated\":true,\"HandleSourceTableAltered\":true},
\"PostProcessingRules\":null}",
    "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
    "TableMappings": "{\"rules\":[{\"rule-type\":\"selection\",\"rule-id\":
\"969761702\",\"rule-name\":\"969761702\",\"object-locator\":{\"schema-name\":\"%table
\",\"table-name\":\"%example\"},\"rule-action\":\"exclude\",\"filters\":[]}]}",
    "TargetEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:ABR8LBOQB3CZY33F7XV253NAJVBNPK6MJQVFVQA"
}
```

AwsDynamoDB sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsDynamoDB` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsDynamoDbTable

Ob `AwsDynamoDbTable` jek memberikan detail tentang tabel Amazon DynamoDB.

Berikut ini adalah contoh `AwsDynamoDbTable` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsDynamoDbTable` atribut, lihat AwsDynamoDbTableDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsDynamoDbTable": {
    "AttributeDefinitions": [
        {
            "AttributeName": "attribute1",
            "AttributeType": "value 1"
        },
        {
            "AttributeName": "attribute2",
```

```
            "AttributeType": "value 2"
        },
        {
            "AttributeName": "attribute3",
            "AttributeType": "value 3"
        }
    ],
    "BillingModeSummary": {
        "BillingMode": "PAY_PER_REQUEST",
        "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
    },
    "CreationDateTime": "2019-12-03T15:23:10.248Z",
    "DeletionProtectionEnabled": true,
    "GlobalSecondaryIndexes": [
        {
            "Backfilling": false,
            "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
            "IndexName": "standardsControlArnIndex",
            "IndexSizeBytes": 1862513,
            "IndexStatus": "ACTIVE",
            "ItemCount": 20,
            "KeySchema": [
                {
                    "AttributeName": "City",
                    "KeyType": "HASH"
                },
                {
                    "AttributeName": "Date",
                    "KeyType": "RANGE"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
            "ProvisionedThroughput": {
                "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
                "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
                "NumberOfDecreasesToday": 0,
                "ReadCapacityUnits": 100,
                "WriteCapacityUnits": 50
            },
        }
```

```
    ],
    "GlobalTableVersion": "V1",
    "ItemCount": 2705,
    "KeySchema": [
        {
            "AttributeName": "zipcode",
            "KeyType": "HASH"
        }
     ],
     "LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
     "LatestStreamLabel": "2019-12-03T23:23:10.248",
     "LocalSecondaryIndexes": [
        {
            "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
            "IndexName": "CITY_DATE_INDEX_NAME",
            "KeySchema": [
                {
                    "AttributeName": "zipcode",
                    "KeyType": "HASH"
                }
            ],
            "Projection": {
                "NonKeyAttributes": ["predictorName"],
                "ProjectionType": "ALL"
            },
        }
    ],
    "ProvisionedThroughput": {
        "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
        "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
        "NumberOfDecreasesToday": 0,
        "ReadCapacityUnits": 100,
        "WriteCapacityUnits": 50
    },
    "Replicas": [
        {
            "GlobalSecondaryIndexes":[
                {
                    "IndexName": "CITY_DATE_INDEX_NAME",
                    "ProvisionedThroughputOverride": {
                        "ReadCapacityUnits": 10
                    }
```

```
                }
            ],
            "KmsMasterKeyId" : "KmsKeyId"
            "ProvisionedThroughputOverride": {
                "ReadCapacityUnits": 10
            },
            "RegionName": "regionName",
            "ReplicaStatus": "CREATING",
            "ReplicaStatusDescription": "replicaStatusDescription"
        }
    ],
    "RestoreSummary" : {
        "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
backup/backup1",
        "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
        "RestoreDateTime": "2020-06-22T17:40:12.322Z",
        "RestoreInProgress": true
    },
    "SseDescription": {
        "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
        "Status": "ENABLED",
        "SseType": "KMS",
        "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
    },
    "StreamSpecification" : {
        "StreamEnabled": true,
        "StreamViewType": "NEW_IMAGE"
    },
    "TableId": "example-table-id-1",
    "TableName": "example-table",
    "TableSizeBytes": 1862513,
    "TableStatus": "ACTIVE"
}
```

AwsEc2 sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEc2` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihat[AWS Format Penemuan Keamanan (ASFF)](#).

AwsEc2ClientVpnEndpoint

Ob `AwsEc2ClientVpnEndpoint` jek memberikan informasi tentang AWS Client VPN titik akhir. Titik akhir VPN Klien adalah sumber daya yang Anda buat dan konfigurasikan untuk mengaktifkan dan mengelola sesi VPN klien. Ini adalah titik terminasi untuk semua sesi VPN klien.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2ClientVpnEndpoint` objek. Untuk melihat deskripsi `AwsEc2ClientVpnEndpoint` atribut, lihat AwsEc2ClientVpnEndpointDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2ClientVpnEndpoint": {
    "AuthenticationOptions": [
        {
            "MutualAuthentication": {
                "ClientRootCertificateChainArn": "arn:aws:acm:us-
east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
            },
            "Type": "certificate-authentication"
        }
    ],
    "ClientCidrBlock": "10.0.0.0/22",
    "ClientConnectOptions": {
        "Enabled": false
    },
    "ClientLoginBannerOptions": {
        "Enabled": false
    },
    "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
    "ConnectionLogOptions": {
        "Enabled": false
    },
    "Description": "test",
    "DnsServer": ["10.0.0.0"],
    "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "SecurityGroupIdSet": [
        "sg-0f7a177b82b443691"
    ],
    "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
    "SessionTimeoutHours": 24,
```

```
    "SplitTunnel": false,
    "TransportProtocol": "udp",
    "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
    "VpnPort": 443
}
```

AwsEc2Eip

Ob `AwsEc2Eip` jek memberikan informasi tentang alamat IP Elastic.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Eip` objek. Untuk melihat deskripsi `AwsEc2Eip` atribut, lihat AwsEc2EipDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Eip": {
    "InstanceId": "instance1",
    "PublicIp": "192.0.2.04",
    "AllocationId": "eipalloc-example-id-1",
    "AssociationId": "eipassoc-example-id-1",
    "Domain": "vpc",
    "PublicIpv4Pool": "anycompany",
    "NetworkBorderGroup": "eu-central-1",
    "NetworkInterfaceId": "eni-example-id-1",
    "NetworkInterfaceOwnerId": "777788889999",
    "PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

Ob `AwsEc2Instance` jek memberikan detail tentang instans Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Instance` objek. Untuk melihat deskripsi `AwsEc2Instance` atribut, lihat AwsEc2InstanceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
    "ImageId": "ami-1234",
    "IpV4Addresses": [ "1.1.1.1" ],
    "IpV6Addresses": [ "2001:db8:1234:1a2b::123" ],
```

```
    "KeyName": "my_keypair",
    "LaunchedAt": "2018-05-08T16:46:19.000Z",
    "MetadataOptions": {
     "HttpEndpoint": "enabled",
     "HttpProtocolIpv6": "enabled",
     "HttpPutResponseHopLimit": 1,
     "HttpTokens": "optional",
     "InstanceMetadataTags": "disabled",
    },
    "Monitoring": {
     "State": "disabled"
    },
    "NetworkInterfaces": [
      {
         "NetworkInterfaceId": "eni-e5aa89a3"
      }
    ],
    "SubnetId": "subnet-123",
    "Type": "i3.xlarge",
    "VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

Ob `AwsEc2LaunchTemplate` jek berisi detail tentang template peluncuran Amazon Elastic Compute Cloud yang menentukan informasi konfigurasi instance.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2LaunchTemplate` objek. Untuk melihat deskripsi `AwsEc2LaunchTemplate` atribut, lihat AwsEc2LaunchTemplateDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2LaunchTemplate": {
    "DefaultVersionNumber": "1",
    "ElasticGpuSpecifications": ["string"],
    "ElasticInferenceAccelerators": ["string"],
    "Id": "lt-0a16e9802800bdd85",
    "ImageId": "ami-0d5eff06f840b45e9",
    "LatestVersionNumber": "1",
    "LaunchTemplateData": {
     "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
```

```
      "Ebs": {
       "DeleteonTermination": true,
       "Encrypted": true,
       "SnapshotId": "snap-01047646ec075f543",
       "VolumeSize": 8,
       "VolumeType:" "gp2"
      }
     }],
     "MetadataOptions": {
      "HttpTokens": "enabled",
      "HttpPutResponseHopLimit" : 1
     },
     "Monitoring": {
      "Enabled": true,
     "NetworkInterfaces": [{
      "AssociatePublicIpAddress" : true,
     }],
    "LaunchTemplateName": "string",
    "LicenseSpecifications": ["string"],
    "SecurityGroupIds": ["sg-01fce87ad6e019725"],
    "SecurityGroups": ["string"],
    "TagSpecifications": ["string"]
}
```

AwsEc2NetworkAcl

Ob `AwsEc2NetworkAcl` jek berisi detail tentang daftar kontrol akses jaringan (ACL) Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2NetworkAcl` objek. Untuk melihat deskripsi `AwsEc2NetworkAcl` atribut, lihat AwsEc2NetworkAclDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2NetworkAcl": {
    "IsDefault": false,
    "NetworkAclId": "acl-1234567890abcdef0",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234abcd",
    "Associations": [{
        "NetworkAclAssociationId": "aclassoc-abcd1234",
        "NetworkAclId": "acl-021345abcdef6789",
        "SubnetId": "subnet-abcd1234"
```

```
    }],
    "Entries": [{
         "CidrBlock": "10.24.34.0/23",
         "Egress": true,
         "IcmpTypeCode": {
             "Code": 10,
             "Type": 30
         },
         "Ipv6CidrBlock": "2001:DB8::/32",
         "PortRange": {
             "From": 20,
             "To": 40
         },
         "Protocol": "tcp",
         "RuleAction": "allow",
         "RuleNumber": 100
    }]
}
```

AwsEc2NetworkInterface

Ob `AwsEc2NetworkInterface` jek menyediakan informasi tentang antarmuka jaringan Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2NetworkInterface` objek. Untuk melihat deskripsi `AwsEc2NetworkInterface` atribut, lihat AwsEc2NetworkInterfaceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2NetworkInterface": {
    "Attachment": {
        "AttachTime": "2019-01-01T03:03:21Z",
        "AttachmentId": "eni-attach-43348162",
        "DeleteOnTermination": true,
        "DeviceIndex": 123,
        "InstanceId": "i-1234567890abcdef0",
        "InstanceOwnerId": "123456789012",
        "Status": 'ATTACHED'
    },
    "SecurityGroups": [
        {
            "GroupName": "my-security-group",
```

```
            "GroupId": "sg-903004f8"
        },
    ],
    "NetworkInterfaceId": 'eni-686ea200',
    "SourceDestCheck": false
}
```

AwsEc2RouteTable

Ob `AwsEc2RouteTable` jek menyediakan informasi tentang tabel rute Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2RouteTable` objek. Untuk melihat deskripsi `AwsEc2RouteTable` atribut, lihat AwsEc2RouteTableDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2RouteTable": {
    "AssociationSet": [{
     "AssociationSet": {
      "State": "associated"
        },
     "Main": true,
     "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
     "RouteTableId": "rtb-0a59bde9cf2548e34",
    }],
    "PropogatingVgwSet": [],
    "RouteTableId": "rtb-0a59bde9cf2548e34",
    "RouteSet": [
     {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
     },
     {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
     }
    ],
    "VpcId": "vpc-0c250a5c33f51d456"
```

```
}
```

AwsEc2SecurityGroup

Ob `AwsEc2SecurityGroup` jek menggambarkan grup keamanan Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2SecurityGroup` objek. Untuk melihat deskripsi `AwsEc2SecurityGroup` atribut, lihat AwsEc2SecurityGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2SecurityGroup": {
    "GroupName": "MySecurityGroup",
    "GroupId": "sg-903004f8",
    "OwnerId": "123456789012",
    "VpcId": "vpc-1a2b3c4d",
    "IpPermissions": [
        {
            "IpProtocol": "-1",
            "IpRanges": [],
            "UserIdGroupPairs": [
                {
                    "UserId": "123456789012",
                    "GroupId": "sg-903004f8"
                }
            ],
            "PrefixListIds": [
                {"PrefixListId": "pl-63a5400a"}
            ]
        },
        {
            "PrefixListIds": [],
            "FromPort": 22,
            "IpRanges": [
                {
                    "CidrIp": "203.0.113.0/24"
                }
            ],
            "ToPort": 22,
            "IpProtocol": "tcp",
            "UserIdGroupPairs": []
        }
```

```
    ]
}
```

AwsEc2Subnet

Ob `AwsEc2Subnet` jek menyediakan informasi tentang subnet di Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Subnet` objek. Untuk melihat deskripsi `AwsEc2Subnet` atribut, lihat AwsEc2SubnetDetails di Referensi AWS Security Hub API.

Contoh

```
AwsEc2Subnet: {
    "AssignIpv6AddressOnCreation": false,
    "AvailabilityZone": "us-west-2c",
    "AvailabilityZoneId": "usw2-az3",
    "AvailableIpAddressCount": 8185,
    "CidrBlock": "10.0.0.0/24",
    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
        "AssociationId": "subnet-cidr-assoc-EXAMPLE",
        "Ipv6CidrBlock": "2001:DB8::/32",
        "CidrBlockState": "associated"
   }]
}
```

AwsEc2TransitGateway

Ob `AwsEc2TransitGateway` jek memberikan detail tentang gateway transit Amazon EC2 yang menghubungkan awan pribadi virtual (VPC) dan jaringan lokal Anda.

Berikut ini adalah contoh `AwsEc2TransitGateway` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsEc2TransitGateway` atribut, lihat AwsEc2TransitGatewayDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2TransitGateway": {
 "AmazonSideAsn": 65000,
 "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "AutoAcceptSharedAttachments": "disable",
 "DefaultRouteTableAssociation": "enable",
 "DefaultRouteTablePropagation": "enable",
 "Description": "sample transit gateway",
 "DnsSupport": "enable",
 "Id": "tgw-042ae6bf7a5c126c3",
 "MulticastSupport": "disable",
 "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
 "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
 "VpnEcmpSupport": "enable"
}
```

AwsEc2Volume

Ob `AwsEc2Volume` jek memberikan rincian tentang volume Amazon EC2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Volume` objek. Untuk melihat deskripsi `AwsEc2Volume` atribut, lihat AwsEc2VolumeDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Volume": {
    "Attachments": [
      {
        "AttachTime": "2017-10-17T14:47:11Z",
        "DeleteOnTermination": true,
        "InstanceId": "i-123abc456def789g",
        "Status": "attached"
      }
     ],
    "CreateTime": "2020-02-24T15:54:30Z",
    "Encrypted": true,
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "Size": 80,
    "SnapshotId": "",
    "Status": "available"
}
```

AwsEc2Vpc

Ob `AwsEc2Vpc` jek memberikan rincian tentang Amazon EC2 VPC.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2Vpc` objek. Untuk melihat deskripsi `AwsEc2Vpc` atribut, lihat AwsEc2VpcDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2Vpc": {
    "CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlock": "192.0.2.0/24",
            "CidrBlockState": "associated"
        }
    ],
    "DhcpOptionsId": "dopt-4e42ce28",
    "Ipv6CidrBlockAssociationSet": [
        {
            "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
            "CidrBlockState": "associated",
            "Ipv6CidrBlock": "192.0.2.0/24"
       }

    ],
    "State": "available"
}
```

AwsEc2VpcEndpointService

Ob `AwsEc2VpcEndpointService` jek berisi detail tentang konfigurasi layanan untuk layanan titik akhir VPC.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2VpcEndpointService` objek. Untuk melihat deskripsi `AwsEc2VpcEndpointService` atribut, lihat AwsEc2VpcEndpointServiceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2VpcEndpointService": {
    "ServiceType": [
      {
```

```
        "ServiceType": "Interface"
      }
    ],
    "ServiceId": "vpce-svc-example1",
    "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
    "ServiceState": "Available",
    "AvailabilityZones": [
      "us-east-1"
    ],
    "AcceptanceRequired": true,
    "ManagesVpcEndpoints": false,
    "NetworkLoadBalancerArns": [
      "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-
load-balancer/example1"
    ],
    "GatewayLoadBalancerArns": [],
    "BaseEndpointDnsNames": [
      "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
    ],
    "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

Ob `AwsEc2VpcPeeringConnection` jek memberikan rincian tentang koneksi jaringan antara dua VPC.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEc2VpcPeeringConnection` objek. Untuk melihat deskripsi `AwsEc2VpcPeeringConnection` atribut, lihat AwsEc2VpcPeeringConnectionDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEc2VpcPeeringConnection": {
 "AccepterVpcInfo": {
  "CidrBlock": "10.0.0.0/28",
  "CidrBlockSet": [{
   "CidrBlock": "10.0.0.0/28"
  }],
  "Ipv6CidrBlockSet": [{
   "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
  }],
```

```
   "OwnerId": "012345678910",
   "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
   },
   "Region": "us-west-2",
   "VpcId": "vpc-i123456"
  },
  "ExpirationTime": "2022-02-18T15:31:53.161Z",
  "RequesterVpcInfo": {
   "CidrBlock": "192.168.0.0/28",
   "CidrBlockSet": [{
    "CidrBlock": "192.168.0.0/28"
   }],
   "Ipv6CidrBlockSet": [{
    "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
   }],
   "OwnerId": "012345678910",
   "PeeringOptions": {
    "AllowDnsResolutionFromRemoteVpc": true,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
    "AllowEgressFromLocalVpcToRemoteClassicLink": true
   },
   "Region": "us-west-2",
   "VpcId": "vpc-i123456"
  },
  "Status": {
   "Code": "initiating-request",
   "Message": "Active"
  },
  "VpcPeeringConnectionId": "pcx-1a2b3c4d"
}
```


AwsEcr sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEcr` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsEcrContainerImage

Ob `AwsEcrContainerImage` jek memberikan informasi tentang gambar Amazon ECR.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcrContainerImage` objek. Untuk melihat deskripsi `AwsEcrContainerImage` atribut, lihat AwsEcrContainerImageDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

Ob `AwsEcrRepository` jek menyediakan informasi tentang repositori Amazon Elastic Container Registry.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcrRepository` objek. Untuk melihat deskripsi `AwsEcrRepository` atribut, lihat AwsEcrRepositoryDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEcs` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsEcsCluster

Ob `AwsEcsCluster` jek menyediakan detail tentang cluster Amazon Elastic Container Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsCluster` objek. Untuk melihat deskripsi `AwsEcsCluster` atribut, lihat AwsEcsClusterDetails di Referensi AWS Security Hub API.

Contoh

```
    "AwsEcsCluster": {
        "CapacityProviders": [],
        "ClusterSettings": [
            {
                "Name": "containerInsights",
                "Value": "enabled"
            }
        ],
        "Configuration": {
            "ExecuteCommandConfiguration": {
                "KmsKeyId": "kmsKeyId",
                "LogConfiguration": {
                    "CloudWatchEncryptionEnabled": true,
                    "CloudWatchLogGroupName": "cloudWatchLogGroupName",
                    "S3BucketName": "s3BucketName",
                    "S3EncryptionEnabled": true,
                    "S3KeyPrefix": "s3KeyPrefix"
                },
                "Logging": "DEFAULT"
            }
        }
        "DefaultCapacityProviderStrategy": [
            {
                "Base": 0,
                "CapacityProvider": "capacityProvider",
                "Weight": 1
            }
        ]
    }
```

AwsEcsContainer

Ob `AwsEcsContainer` jek berisi detail tentang wadah Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsContainer` objek. Untuk melihat deskripsi `AwsEcsContainer` atribut, lihat AwsEcsContainerDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

AwsEcsService

Ob `AwsEcsService` jek memberikan rincian tentang layanan dalam cluster Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsService` objek. Untuk melihat deskripsi `AwsEcsService` atribut, lihat AwsEcsServiceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEcsService": {
    "CapacityProviderStrategy": [
        {
            "Base": 12,
            "CapacityProvider": "",
            "Weight": ""
        }
    ],
    "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
    "DeploymentConfiguration": {
        "DeploymentCircuitBreaker": {
            "Enable": false,
```

```
            "Rollback": false
        },
        "MaximumPercent": 200,
        "MinimumHealthyPercent": 100
    },
    "DeploymentController": "",
    "DesiredCount": 1,
    "EnableEcsManagedTags": false,
    "EnableExecuteCommand": false,
    "HealthCheckGracePeriodSeconds": 1,
    "LaunchType": "FARGATE",
    "LoadBalancers": [
        {
            "ContainerName": "",
            "ContainerPort": 23,
            "LoadBalancerName": "",
            "TargetGroupArn": ""
        }
    ],
    "Name": "sample-app-service",
    "NetworkConfiguration": {
        "AwsVpcConfiguration": {
            "Subnets": [
                "Subnet-example1",
                "Subnet-example2"
            ],
        "SecurityGroups": [
                "Sg-0ce48e9a6e5b457f5"
        ],
        "AssignPublicIp": "ENABLED"
        }
    },
    "PlacementConstraints": [
        {
            "Expression": "",
            "Type": ""
        }
    ],
    "PlacementStrategies": [
        {
            "Field": "",
            "Type": ""
        }
    ],
```

```
    "PlatformVersion": "LATEST",
    "PropagateTags": "",
    "Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/
ServiceRoleForECS",
    "SchedulingStrategy": "REPLICA",
    "ServiceName": "sample-app-service",
    "ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/
sample-app-service",
    "ServiceRegistries": [
        {
            "ContainerName": "",
            "ContainerPort": 1212,
            "Port": 1221,
            "RegistryArn": ""
        }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-
taskdef:1"
}
```

AwsEcsTask

Ob `AwsEcsTask` jek memberikan detail tentang tugas Amazon ECS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsTask` objek. Untuk melihat deskripsi `AwsEcsTask` atribut, lihat AwsEcsTask di Referensi AWS Security Hub API.

Contoh

```
"AwsEcsTask": {
 "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
 "CreatedAt": "1557134011644",
 "Group": "service:fargate-service",
 "StartedAt": "1557134011644",
 "StartedBy": "ecs-svc/1234567890123456789",
 "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-
fargate:2",
 "Version": 3,
 "Volumes": [{
  "Name": "string",
  "Host": {
   "SourcePath": "string"
  }
```

```
 }],
 "Containers": {
  "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
   "ContainerPath": "/mnt/etc",
   "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
 }
}
```

AwsEcsTaskDefinition

Ob `AwsEcsTaskDefinition` jek berisi detail tentang definisi tugas. Definisi tugas menjelaskan definisi wadah dan volume tugas Amazon Elastic Container Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEcsTaskDefinition` objek. Untuk melihat deskripsi `AwsEcsTaskDefinition` atribut, lihat AwsEcsTaskDefinitionDetails di Referensi AWS Security Hub API.

Contoh

```
    "AwsEcsTaskDefinition": {
        "ContainerDefinitions": [
            {
                "Command": ['ruby', 'hi.rb'],
                "Cpu":128,
                "Essential": true,
                "HealthCheck": {
                    "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],
                    "Interval": 10,
                    "Retries": 3,
                    "StartPeriod": 5,
                    "Timeout": 20
                },
                "Image": "tongueroo/sinatra:latest",
                "Interactive": true,
                "Links": [],
                "LogConfiguration": {
                    "LogDriver": "awslogs",
                    "Options": {
```

```
                    "awslogs-group": "/ecs/sinatra-hi",
                    "awslogs-region": "ap-southeast-1",
                    "awslogs-stream-prefix": "ecs"
                },
                "SecretOptions": []

            },
            "MemoryReservation": 128,
            "Name": "web",
            "PortMappings": [
                {
                    "ContainerPort": 4567,
                    "HostPort":4567,
                    "Protocol": "tcp"
                }
            ],
            "Privileged": true,
            "StartTimeout": 10,
            "StopTimeout": 100,
        }
    ],
    "Family": "sinatra-hi",
    "NetworkMode": "host",
    "RequiresCompatibilities": ["EC2"],
    "Status": "ACTIVE",
    "TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}
```

AwsEfs sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEfs` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsEfsAccessPoint

Ob `AwsEfsAccessPoint` jek memberikan rincian tentang file yang disimpan di Amazon Elastic File System.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEfsAccessPoint` objek. Untuk melihat deskripsi `AwsEfsAccessPoint` atribut, lihat AwsEfsAccessPointDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEfsAccessPoint": {
 "AccessPointId": "fsap-05c4c0e79ba0b118a",
 "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/
fsap-05c4c0e79ba0b118a",
 "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
 "FileSystemId": "fs-0f8137f731cb32146",
 "PosixUser": {
  "Gid": "1000",
  "SecondaryGids": ["0", "4294967295"],
  "Uid": "1234"
 },
 "RootDirectory": {
  "CreationInfo": {
   "OwnerGid": "1000",
   "OwnerUid": "1234",
   "Permissions": "777"
  },
  "Path": "/tmp/example"
 }
}
```

AwsEks sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEks` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsEksCluster

Ob `AwsEksCluster` jek memberikan detail tentang cluster Amazon EKS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEksCluster` objek. Untuk melihat deskripsi `AwsEksCluster` atribut, lihat AwsEksClusterDetails di Referensi AWS Security Hub API.

Contoh

```
{
  "AwsEksCluster": {
```

```
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-
ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    },
    "Logging": {
      "ClusterLogging": [
        {
          "Types": [
            "api",
            "audit",
            "authenticator",
            "controllerManager",
            "scheduler"
          ],
          "Enabled": true
        }
      ]
    },
    "Status": "CREATING",
    "CertificateAuthorityData": {},
  }
}
```

AwsElasticBeanstalk sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsElasticBeanstalk` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsElasticBeanstalkEnvironment

Ob `AwsElasticBeanstalkEnvironment` jek berisi detail tentang AWS Elastic Beanstalk lingkungan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElasticBeanstalkEnvironment` objek. Untuk melihat deskripsi `AwsElasticBeanstalkEnvironment` atribut, lihat AwsElasticBeanstalkEnvironmentDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "MyApplication",
    "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
    "DateCreated": "2021-04-30T01:38:01.090Z",
    "DateUpdated": "2021-04-30T01:38:01.090Z",
    "Description": "Example description of my awesome application",
    "EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
    "EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
    "EnvironmentId": "e-abcd1234",
    "EnvironmentLinks": [
        {
            "EnvironmentName": "myexampleapp-env",
            "LinkName": "myapplicationLink"
        }
    ],
    "EnvironmentName": "myapplication-env",
    "OptionSettings": [
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "BatchSize",
            "Value": "100"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "Timeout",
            "Value": "600"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
```

```
            "OptionName": "BatchSizeType",
            "Value": "Percentage"
        },
        {
            "Namespace": "aws:elasticbeanstalk:command",
            "OptionName": "IgnoreHealthCheck",
            "Value": "false"
        },
        {
            "Namespace": "aws:elasticbeanstalk:application",
            "OptionName": "Application Healthcheck URL",
            "Value": "TCP:80"
        }
    ],
    "PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
 running on 64bit Amazon Linux/2.7.7",
    "SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
    "Status": "Ready",
    "Tier": {
        "Name": "WebServer"
       "Type": "Standard"
       "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
}
```

AwsElasticSearch sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsElasticSearch` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsElasticSearchDomain

Ob `AwsElasticSearchDomain` jek memberikan rincian tentang domain OpenSearch Layanan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElasticSearchDomain` objek. Untuk melihat deskripsi `AwsElasticSearchDomain` atribut, lihat AwsElasticSearchDomainDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsElasticSearchDomain": {
    "AccessPolicies": "string",
    "DomainStatus": {
           "DomainId": "string",
           "DomainName": "string",
           "Endpoint": "string",
           "Endpoints": {
                  "string": "string"
           }
    },
    "DomainEndpointOptions": {
           "EnforceHTTPS": boolean,
           "TLSSecurityPolicy": "string"
    },
    "ElasticsearchClusterConfig": {
           "DedicatedMasterCount": number,
           "DedicatedMasterEnabled": boolean,
           "DedicatedMasterType": "string",
           "InstanceCount": number,
           "InstanceType": "string",
           "ZoneAwarenessConfig": {
                  "AvailabilityZoneCount": number
           },
           "ZoneAwarenessEnabled": boolean
    },
    "ElasticsearchVersion": "string",
    "EncryptionAtRestOptions": {
           "Enabled": boolean,
           "KmsKeyId": "string"
    },
    "LogPublishingOptions": {
           "AuditLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "IndexSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
           },
           "SearchSlowLogs": {
                  "CloudWatchLogsLogGroupArn": "string",
                  "Enabled": boolean
```

```
            }
    },
    "NodeToNodeEncryptionOptions": {
            "Enabled": boolean
    },
    "ServiceSoftwareOptions": {
            "AutomatedUpdateDate": "string",
            "Cancellable": boolean,
            "CurrentVersion": "string",
            "Description": "string",
            "NewVersion": "string",
            "UpdateAvailable": boolean,
            "UpdateStatus": "string"
    },
    "VPCOptions": {
            "AvailabilityZones": [
                  "string"
            ],
            "SecurityGroupIds": [
                  "string"
            ],
            "SubnetIds": [
                  "string"
            ],
           "VPCId": "string"
    }
}
```

AwsElb sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsElb` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsElbLoadBalancer

Ob `AwsElbLoadBalancer` jek berisi detail tentang Classic Load Balancer.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElbLoadBalancer` objek. Untuk melihat deskripsi `AwsElbLoadBalancer` atribut, lihat AwsElbLoadBalancerDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsElbLoadBalancer": {
    "AvailabilityZones": ["us-west-2a"],
    "BackendServerDescriptions": [
         {
            "InstancePort": 80,
            "PolicyNames": ["doc-example-policy"]
        }
    ],
    "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
    "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-
west-2.elb.amazonaws.com",
    "CreatedTime": "2020-08-03T19:22:44.637Z",
    "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/png",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    },
    "Instances": [
        {
            "InstanceId": "i-example"
        }
    ],
    "ListenerDescriptions": [
        {
            "Listener": {
                "InstancePort": 443,
                "InstanceProtocol": "HTTPS",
                "LoadBalancerPort": 443,
                "Protocol": "HTTPS",
                "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
            },
            "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
        }
    ],
    "LoadBalancerAttributes": {
        "AccessLog": {
            "EmitInterval": 60,
            "Enabled": true,
            "S3BucketName": "amzn-s3-demo-bucket",
```

```
            "S3BucketPrefix": "doc-example-prefix"
        },
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "ConnectionSettings": {
            "IdleTimeout": 30
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "AdditionalAttributes": [{
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }]

    },
    "LoadBalancerName": "example-load-balancer",
    "Policies": {
        "AppCookieStickinessPolicies": [
            {
                "CookieName": "",
                "PolicyName": ""
            }
        ],
        "LbCookieStickinessPolicies": [
            {
                "CookieExpirationPeriod": 60,
                "PolicyName": "my-example-cookie-policy"
            }
        ],
        "OtherPolicies": [
            "my-PublicKey-policy",
            "my-authentication-policy",
            "my-SSLNegotiation-policy",
            "my-ProxyProtocol-policy",
            "ELBSecurityPolicy-2015-03"
        ]
    },
    "Scheme": "internet-facing",
    "SecurityGroups": ["sg-example"],
    "SourceSecurityGroup": {
        "GroupName": "my-elb-example-group",
```

```
        "OwnerAlias": "444455556666"
    },
    "Subnets": ["subnet-example"],
    "VpcId": "vpc-a01106c2"
}
```

AwsElbv2LoadBalancer

Ob `AwsElbv2LoadBalancer` jek memberikan informasi tentang penyeimbang beban.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsElbv2LoadBalancer` objek. Untuk melihat deskripsi `AwsElbv2LoadBalancer` atribut, lihat AwsElbv2LoadBalancerDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsElbv2LoadBalancer": {
                        "AvailabilityZones": {
                            "SubnetId": "string",
                            "ZoneName": "string"
                        },
                        "CanonicalHostedZoneId": "string",
                        "CreatedTime": "string",
                        "DNSName": "string",
                        "IpAddressType": "string",
                        "LoadBalancerAttributes": [
                            {
                                "Key": "string",
                                "Value": "string"
                            }
                        ],
                        "Scheme": "string",
                        "SecurityGroups": [ "string" ],
                        "State": {
                            "Code": "string",
                            "Reason": "string"
                        },
                        "Type": "string",
                        "VpcId": "string"
                    }
```

AwsEventBridge sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsEventBridge` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsEventSchemasRegistry

Ob `AwsEventSchemasRegistry` jek menyediakan informasi tentang registri EventBridge skema Amazon. Skema mendefinisikan struktur peristiwa yang dikirim ke EventBridge. Pendaftar skema adalah wadah yang mengumpulkan dan secara logis mengelompokkan skema Anda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEventSchemasRegistry` objek. Untuk melihat deskripsi `AwsEventSchemasRegistry` atribut, lihat AwsEventSchemasRegistry di Referensi AWS Security Hub API.

Contoh

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

Ob `AwsEventsEndpoint` jek menyediakan informasi tentang titik akhir EventBridge global Amazon. Titik akhir dapat meningkatkan ketersediaan aplikasi Anda dengan membuatnya Regional-fault toleran.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEventsEndpoint` objek. Untuk melihat deskripsi `AwsEventsEndpoint` atribut, lihat AwsEventsEndpointDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEventsEndpoint": {
    "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
    "Description": "This is a sample endpoint.",
    "EndpointId": "04k1exajoy.veo",
```

```
    "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
    "EventBuses": [
        {
            "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
        },
        {
            "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
        }
    ],
    "Name": "my-endpoint",
    "ReplicationConfig": {
        "State": "ENABLED"
    },
    "RoleArn": "arn:aws:iam::123456789012:role/service-role/
Amazon_EventBridge_Invoke_Event_Bus_1258925394",
    "RoutingConfig": {
        "FailoverConfig": {
            "Primary": {
                "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
            },
            "Secondary": {
                "Route": "us-east-2"
            }
        }
    },
    "State": "ACTIVE"
}
```

AwsEventsEventbus

Ob `AwsEventsEventbus` jek menyediakan informasi tentang titik akhir EventBridge global Amazon. Titik akhir dapat meningkatkan ketersediaan aplikasi Anda dengan membuatnya Regional-fault toleran.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsEventsEventbus` objek. Untuk melihat deskripsi `AwsEventsEventbus` atribut, lihat AwsEventsEventbusDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsEventsEventbus":
    "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
```

```
    "Name": "my-event-bus",
    "Policy": "{\"Version\":\"2012-10-17\",       \"Statement\":[{\"Sid
\":\"AllowAllAccountsFromOrganizationToPutEvents\",\"Effect\":\"Allow
\",\"Principal\":\"*\",\"Action\":\"events:PutEvents\",\"Resource\":
\"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\",\"Condition
\":{\"StringEquals\":{\"aws:PrincipalOrgID\":\"o-ki7yjtkjv5\"}}},{\"Sid\":
\"AllowAccountToManageRulesTheyCreated\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
\"arn:aws:iam::123456789012:root\"},\"Action\":[\"events:PutRule\",\"events:PutTargets
\",\"events:DeleteRule\",\"events:RemoveTargets\",\"events:DisableRule\",
\"events:EnableRule\",\"events:TagResource\",\"events:UntagResource\",
\"events:DescribeRule\",\"events:ListTargetsByRule\",\"events:ListTagsForResource\"],
\"Resource\":\"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\",\"Condition\":
{\"StringEqualsIfExists\":{\"events:creatorAccount\":\"123456789012\"}}}]}"
```


AwsGuardDuty sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsGuardDuty` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsGuardDutyDetector

Ob `AwsGuardDutyDetector` jek memberikan informasi tentang GuardDuty detektor Amazon. Detektor adalah objek yang mewakili GuardDuty layanan. Detektor diperlukan GuardDuty untuk menjadi operasional.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsGuardDutyDetector` objek. Untuk melihat deskripsi `AwsGuardDutyDetector` atribut, lihat AwsGuardDutyDetector di Referensi AWS Security Hub API.

Contoh


```
"AwsGuardDutyDetector": {
    "FindingPublishingFrequency": "SIX_HOURS",
    "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/
guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
    "Status": "ENABLED",
    "DataSources": {
        "CloudTrail": {
            "Status": "ENABLED"
        },
```

```
        "DnsLogs": {
            "Status": "ENABLED"
        },
        "FlowLogs": {
            "Status": "ENABLED"
        },
        "S3Logs": {
             "Status": "ENABLED"
         },
         "Kubernetes": {
             "AuditLogs": {
                "Status": "ENABLED"
             }
         },
         "MalwareProtection": {
             "ScanEc2InstanceWithFindings": {
                "EbsVolumes": {
                    "Status": "ENABLED"
                 }
             },
            "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-
protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
         }
    }
}
```

Awslam sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsIam` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsIamAccessKey

Ob `AwsIamAccessKey` jek berisi detail tentang kunci akses IAM yang terkait dengan temuan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamAccessKey` objek. Untuk melihat deskripsi `AwsIamAccessKey` atribut, lihat AwsIamAccessKeyDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsIamAccessKey": {
```

```
                    "AccessKeyId": "string",
                    "AccountId": "string",
                    "CreatedAt": "string",
                    "PrincipalId": "string",
                    "PrincipalName": "string",
                    "PrincipalType": "string",
                    "SessionContext": {
                        "Attributes": {
                            "CreationDate": "string",
                            "MfaAuthenticated": boolean
                        },
                        "SessionIssuer": {
                            "AccountId": "string",
                            "Arn": "string",
                            "PrincipalId": "string",
                            "Type": "string",
                            "UserName": "string"
                        }
                    },
                    "Status": "string"
                }
```

AwsIamGroup

Ob `AwsIamGroup` jek berisi detail tentang grup IAM.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamGroup` objek. Untuk melihat deskripsi `AwsIamGroup` atribut, lihat AwsIamGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsIamGroup": {
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",
            "PolicyName": "ExampleManagedAccess",
        }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
```

```
        {
            "PolicyName": "ExampleGroupPolicy"
        }
    ],
    "Path": "/"
}
```

AwsIamPolicy

Ob `AwsIamPolicy` jek mewakili kebijakan izin IAM.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamPolicy` objek. Untuk melihat deskripsi `AwsIamPolicy` atribut, lihat AwsIamPolicyDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsIamPolicy": {
    "AttachmentCount": 1,
    "CreateDate": "2017-09-14T08:17:29.000Z",
    "DefaultVersionId": "v1",
    "Description": "Example IAM policy",
    "IsAttachable": true,
    "Path": "/",
    "PermissionsBoundaryUsageCount": 5,
    "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
    "PolicyName": "EXAMPLE-MANAGED-POLICY",
    "PolicyVersionList": [
        {
            "VersionId": "v1",
            "IsDefaultVersion": true,
            "CreateDate": "2017-09-14T08:17:29.000Z"
        }
    ],
    "UpdateDate": "2017-09-14T08:17:29.000Z"
}
```

AwsIamRole

Ob `AwsIamRole` jek berisi informasi tentang peran IAM, termasuk semua kebijakan peran.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamRole` objek. Untuk melihat deskripsi `AwsIamRole` atribut, lihat AwsIamRoleDetails di Referensi AWS Security Hub API.

Contoh


```
"AwsIamRole": {
    "AssumeRolePolicyDocument": "{'Version': '2012-10-17',       'Statement':
 [{'Effect': 'Allow','Action': 'sts:AssumeRole'}]}",
    "AttachedManagedPolicies": [
        {
            "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
            "PolicyName": "Example policy 1"
        },
        {
            "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
            "PolicyName": "Example policy 2"
        }
        ],
        "CreateDate": "2020-03-14T07:19:14.000Z",
        "InstanceProfileList": [
            {
                "Arn": "arn:aws:iam::333333333333:ExampleProfile",
                "CreateDate": "2020-03-11T00:02:27Z",
                "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
                "InstanceProfileName": "ExampleInstanceProfile",
                "Path": "/",
                "Roles": [
                    {
                       "Arn": "arn:aws:iam::444455556666:role/example-role",
                        "AssumeRolePolicyDocument": "",
                        "CreateDate": "2020-03-11T00:02:27Z",
                        "Path": "/",
                        "RoleId": "AROAJ52OTH4H7LEXAMPLE",
                        "RoleName": "example-role",
                    }
                ]
            }
        ],
        "MaxSessionDuration": 3600,
        "Path": "/",
        "PermissionsBoundary": {
            "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
            "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
        },
        "RoleId": "AROA4TPS3VLEXAMPLE",
        "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
        "RolePolicyList": [
```

```
            {
                "PolicyName": "Example role policy"
            }
        ]
    }
```

AwsIamUser

Ob `AwsIamUser` jek memberikan informasi tentang pengguna.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsIamUser` objek. Untuk melihat deskripsi `AwsIamUser` atribut, lihat AwsIamUserDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsIamUser": {
    "AttachedManagedPolicies": [
        {
            "PolicyName": "ExamplePolicy",
            "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
        }
    ],
    "CreateDate": "2018-01-26T23:50:05.000Z",
    "GroupList": [],
    "Path": "/",
    "PermissionsBoundary" : {
        "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
        "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
    },
    "UserId": "AIDACKCEVSQ6C2EXAMPLE",
    "UserName": "ExampleUser",
    "UserPolicyList": [
        {
            "PolicyName": "InstancePolicy"
        }
    ]
}
```

AwsKinesis sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsKinesis` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsKinesisStream

Ob `AwsKinesisStream` jek ini memberikan rincian tentang Amazon Kinesis Data Streams.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsKinesisStream` objek. Untuk melihat deskripsi `AwsKinesisStream` atribut, lihat AwsKinesisStreamDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsKinesisStream": {
 "Name": "test-vir-kinesis-stream",
 "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",
 "RetentionPeriodHours": 24,
 "ShardCount": 2,
 "StreamEncryption": {
  "EncryptionType": "KMS",
  "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-
ea76007247eb"
 }
}
```

AwsKms sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsKms` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsKmsKey

Ob `AwsKmsKey` jek memberikan detail tentang AWS KMS key.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsKmsKey` objek. Untuk melihat deskripsi `AwsKmsKey` atribut, lihat AwsKmsKeyDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
```

```
                    "CreationDate": "string",
                    "Description": "string",
                    "KeyId": "string",
                    "KeyManager": "string",
                    "KeyRotationStatus": boolean,
                    "KeyState": "string",
                    "Origin": "string"
                }
```

AwsLambda

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsLambda` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsLambdaFunction

Ob `AwsLambdaFunction` jek memberikan rincian tentang konfigurasi fungsi Lambda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsLambdaFunction` objek. Untuk melihat deskripsi `AwsLambdaFunction` atribut, lihat AwsLambdaFunctionDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsLambdaFunction": {
    "Architectures": [
        "x86_64"
    ],
    "Code": {
        "S3Bucket": "amzn-s3-demo-bucket",
        "S3Key": "samplekey",
        "S3ObjectVersion": "2",
        "ZipFile": "myzip.zip"
    },
    "CodeSha256": "1111111111111abcdef",
    "DeadLetterConfig": {
        "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
    },
    "Environment": {
        "Variables": {
```

```
            "Stage": "foobar"
         },
        "Error": {
            "ErrorCode": "Sample-error-code",
            "Message": "Caller principal is a manager."
         }
     },
    "FunctionName": "CheckOut",
    "Handler": "main.py:lambda_handler",
    "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
    "LastModified": "2001-09-11T09:00:00Z",
    "Layers": {
        "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
        "CodeSize": 169
    },
    "PackageType": "Zip",
    "RevisionId": "23",
    "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
    "Runtime": "go1.7",
    "Timeout": 15,
    "TracingConfig": {
        "Mode": "Active"
    },
    "Version": "$LATEST$",
    "VpcConfig": {
        "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
         "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
    },
    "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
    "MemorySize": 2048
}
```

AwsLambdaLayerVersion

Ob `AwsLambdaLayerVersion` jek memberikan rincian tentang versi lapisan Lambda.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsLambdaLayerVersion` objek. Untuk melihat deskripsi `AwsLambdaLayerVersion` atribut, lihat AwsLambdaLayerVersionDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsLambdaLayerVersion": {
```

```
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsMsk` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsMskCluster

Ob `AwsMskCluster` jek menyediakan informasi tentang cluster Amazon Managed Streaming untuk Apache Kafka (Amazon MSK).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsMskCluster` objek. Untuk melihat deskripsi `AwsMskCluster` atribut, lihat AwsMskClusterDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsMskCluster": {
        "ClusterInfo": {
            "ClientAuthentication": {
                "Sasl": {
                    "Scram": {
                        "Enabled": true
                    },
                    "Iam": {
                        "Enabled": true
                    }
                },
                "Tls": {
                    "CertificateAuthorityArnList": [],
                    "Enabled": false
                },
                "Unauthenticated": {
                    "Enabled": false
                }
```

```
            },
            "ClusterName": "my-cluster",
            "CurrentVersion": "K2PWKAKR8XB7XF",
            "EncryptionInfo": {
                "EncryptionAtRest": {
                    "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
                },
                "EncryptionInTransit": {
                    "ClientBroker": "TLS",
                    "InCluster": true
                }
            },
            "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
            "NumberOfBrokerNodes": 3
        }
}
```

AwsNetworkFirewall sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewall` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsNetworkFirewallFirewall

Ob `AwsNetworkFirewallFirewall` jek berisi detail tentang AWS Network Firewall firewall.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallFirewall` objek. Untuk melihat deskripsi `AwsNetworkFirewallFirewall` atribut, lihat AwsNetworkFirewallFirewallDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsNetworkFirewallFirewall": {
    "DeleteProtection": false,
    "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
    "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
```

```
    "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
    "FirewallName": "testfirewall",
    "FirewallPolicyChangeProtection": false,
    "SubnetChangeProtection": false,
    "SubnetMappings": [
        {
            "SubnetId": "subnet-0183481095e588cdc"
        },
        {
            "SubnetId": "subnet-01f518fad1b1c90b0"
        }
    ],
    "VpcId": "vpc-40e83c38"
}
```

AwsNetworkFirewallFirewallPolicy

Ob `AwsNetworkFirewallFirewallPolicy` jek memberikan rincian tentang kebijakan firewall. Kebijakan firewall mendefinisikan perilaku firewall jaringan.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallFirewallPolicy` objek. Untuk melihat deskripsi `AwsNetworkFirewallFirewallPolicy` atribut, lihat AwsNetworkFirewallFirewallPolicyDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsNetworkFirewallFirewallPolicy": {
   "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
        {
            "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/PatchesOnly"
        }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
       {
          "Priority": 1,
          "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1"
       }
```

```
      ]
   },
   "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
   "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
   "FirewallPolicyName": "InitialFirewall",
   "Description": "Initial firewall"
}
```

AwsNetworkFirewallRuleGroup

Ob `AwsNetworkFirewallRuleGroup` jek memberikan rincian tentang grup AWS Network Firewall aturan. Grup aturan digunakan untuk memeriksa dan mengontrol lalu lintas jaringan. Grup aturan stateless berlaku untuk paket individual. Grup aturan stateful berlaku untuk paket dalam konteks arus lalu lintas mereka.

Grup aturan direferensikan dalam kebijakan firewall.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsNetworkFirewallRuleGroup` objek. Untuk melihat deskripsi `AwsNetworkFirewallRuleGroup` atribut, lihat AwsNetworkFirewallRuleGroupDetails di Referensi AWS Security Hub API.

Contoh — grup aturan tanpa kewarganegaraan

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 600,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
    "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
    "RuleGroupName": "Stateless-1"
    "Description": "Example of a stateless rule group",
    "Type": "STATELESS",
    "RuleGroup": {
        "RulesSource": {
            "StatelessRulesAndCustomActions": {
                "CustomActions": [],
                "StatelessRules": [
                    {
                        "Priority": 1,
                        "RuleDefinition": {
                            "Actions": [
```

```
                            "aws:pass"
                        ],
                        "MatchAttributes": {
                            "DestinationPorts": [
                                {
                                    "FromPort": 443,
                                    "ToPort": 443
                                }
                            ],
                            "Destinations": [
                                {
                                    "AddressDefinition": "192.0.2.0/24"
                                }
                            ],
                            "Protocols": [
                                       6
                            ],
                            "SourcePorts": [
                                {
                                    "FromPort": 0,
                                    "ToPort": 65535
                                }
                            ],
                            "Sources": [
                                {
                                     "AddressDefinition": "198.51.100.0/24"
                                }
                            ]
                        }
                    }
                }
            ]
        }
    }
}
```

Contoh — grup aturan stateful

```
"AwsNetworkFirewallRuleGroup": {
    "Capacity": 100,
    "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
```

```
    "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
    "RuleGroupName": "ExampleRuleGroup",
    "Description": "Example of a stateful rule group",
    "Type": "STATEFUL",
    "RuleGroup": {
        "RuleSource": {
            "StatefulRules": [
                {
                    "Action": "PASS",
                    "Header": {
                        "Destination": "Any",
                        "DestinationPort": "443",
                        "Direction": "ANY",
                        "Protocol": "TCP",
                        "Source": "Any",
                        "SourcePort": "Any"
                    },
                    "RuleOptions": [
                        {
                           "Keyword": "sid:1"
                        }
                    ]
                }
            ]
         }
    }
}
```

Berikut ini adalah daftar contoh nilai yang valid untuk `AwsNetworkFirewallRuleGroup` atribut:

- `Action`

  Nilai yang valid: `PASS | DROP | ALERT`

- `Protocol`

  Nilai yang valid: `IP TCP UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP`

- `Flags`

  Nilai yang valid: `FIN SYN RST | PSH | ACK | URG | ECE | CWR`

- `Masks`

Nilai yang valid: `FIN SYN RST | PSH | ACK | URG | ECE | CWR`

AwsOpenSearchService sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsOpenSearchService` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsOpenSearchServiceDomain

Ob `AwsOpenSearchServiceDomain` jek berisi informasi tentang domain OpenSearch Layanan Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsOpenSearchServiceDomain` objek. Untuk melihat deskripsi `AwsOpenSearchServiceDomain` atribut, lihat AwsOpenSearchServiceDomainDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsOpenSearchServiceDomain": {
    "AccessPolicies": "IAM_Id",
    "AdvancedSecurityOptions": {
        "Enabled": true,
        "InternalUserDatabaseEnabled": true,
        "MasterUserOptions": {
            "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
            "MasterUserName": "third-master-use",
            "MasterUserPassword": "some-password"
        }
    },
    "Arn": "arn:aws:Opensearch:us-east-1:111122223333:somedomain",
    "ClusterConfig": {
        "InstanceType": "c5.large.search",
        "InstanceCount": 1,
        "DedicatedMasterEnabled": true,
        "ZoneAwarenessEnabled": false,
        "ZoneAwarenessConfig": {
            "AvailabilityZoneCount": 2
        },
```

```
        "DedicatedMasterType": "c5.large.search",
        "DedicatedMasterCount": 3,
        "WarmEnabled": true,
        "WarmCount": 3,
        "WarmType": "ultrawarm1.large.search"
    },
    "DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-
central-1.es.amazonaws.com",
    "DomainEndpointOptions": {
        "EnforceHTTPS": false,
        "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
        "CustomEndpointCertificateArn": "arn:aws:acm:us-
east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
        "CustomEndpointEnabled": true,
        "CustomEndpoint": "example.com"
    },
    "DomainEndpoints": {
        "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
    },
    "DomainName": "my-domain",
    "EncryptionAtRestOptions": {
        "Enabled": false,
        "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
    },
    "EngineVersion": "7.1",
    "Id": "123456789012",
    "LogPublishingOptions": {
        "IndexSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-index-slow-logs",
            "Enabled": true
        },
        "SearchSlowLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        },
        "AuditLogs": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-
group:/aws/aes/domains/es-slow-logs",
            "Enabled": true
        }
    },
    "NodeToNodeEncryptionOptions": {
```

```
        "Enabled": true
    },
    "ServiceSoftwareOptions": {
        "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
        "Cancellable": false,
        "CurrentVersion": "R20210331",
        "Description": "There is no software update available for this domain.",
        "NewVersion": "OpenSearch_1.0",
        "UpdateAvailable": false,
        "UpdateStatus": "COMPLETED",
        "OptionalDeployment": false
    },
    "VpcOptions": {
        "SecurityGroupIds": [
            "sg-2a3a4a5a"
        ],
        "SubnetIds": [
            "subnet-1a2a3a4a"
        ],
    }
}
```

AwsRds sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsRds` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsRdsDbCluster

Ob `AwsRdsDbCluster` jek memberikan rincian tentang cluster database Amazon RDS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbCluster` objek. Untuk melihat deskripsi `AwsRdsDbCluster` atribut, lihat AwsRdsDbClusterDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbCluster": {
    "ActivityStreamStatus": "stopped",
    "AllocatedStorage": 1,
    "AssociatedRoles": [
        {
```

```
        "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/
AWSServiceRoleForRDS",
        "Status": "PENDING"
        }
    ],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1c",
        "us-east-1e"
    ],
    "BackupRetentionPeriod": 1,
    "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
    "CopyTagsToSnapshot": true,
    "CrossAccountClone": false,
    "CustomEndpoints": [],
    "DatabaseName": "Sample name",
    "DbClusterIdentifier": "database-3",
    "DbClusterMembers": [
        {
        "DbClusterParameterGroupStatus": "in-sync",
        "DbInstanceIdentifier": "database-3-instance-1",
        "IsClusterWriter": true,
        "PromotionTier": 1,
        }
    ],
    "DbClusterOptionGroupMemberships": [],
    "DbClusterParameterGroup": "cluster-parameter-group",
    "DbClusterResourceId": "cluster-example",
    "DbSubnetGroup": "subnet-group",
    "DeletionProtection": false,
    "DomainMemberships": [],
    "Status": "modifying",
    "EnabledCloudwatchLogsExports": [
        "audit",
        "error",
        "general",
        "slowquery"
    ],
    "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
    "Engine": "aurora-mysql",
    "EngineMode": "provisioned",
    "EngineVersion": "5.7.mysql_aurora.2.03.4",
    "HostedZoneId": "ZONE1",
```

```
    "HttpEndpointEnabled": false,
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "MasterUsername": "admin",
    "MultiAz": false,
    "Port": 3306,
    "PreferredBackupWindow": "04:52-05:22",
    "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
    "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example-1"
        }
    ],
}
```

AwsRdsDbClusterSnapshot

Ob `AwsRdsDbClusterSnapshot` jek berisi informasi tentang snapshot cluster Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbClusterSnapshot` objek. Untuk melihat deskripsi `AwsRdsDbClusterSnapshot` atribut, lihat AwsRdsDbClusterSnapshotDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbClusterSnapshot": {
    "AllocatedStorage": 0,
    "AvailabilityZones": [
        "us-east-1a",
        "us-east-1d",
        "us-east-1e"
    ],
    "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
    "DbClusterIdentifier": "database-2",
    "DbClusterSnapshotAttributes": [{
        "AttributeName": "restore",
        "AttributeValues": ["123456789012"]
    }],
```

```
    "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
    "Engine": "aurora",
    "EngineVersion": "5.6.10a",
    "IamDatabaseAuthenticationEnabled": false,
    "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
    "LicenseModel": "aurora",
    "MasterUsername": "admin",
    "PercentProgress": 100,
    "Port": 0,
    "SnapshotCreateTime": "2020-06-22T17:40:12.322Z",
    "SnapshotType": "automated",
    "Status": "available",
    "StorageEncrypted": true,
    "VpcId": "vpc-faf7e380"
}
```

AwsRdsDbInstance

Ob `AwsRdsDbInstance` jek menyediakan detail tentang instance Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbInstance` objek. Untuk melihat deskripsi `AwsRdsDbInstance` atribut, lihat AwsRdsDbInstanceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbInstance": {
    "AllocatedStorage": 20,
    "AssociatedRoles": [],
    "AutoMinorVersionUpgrade": true,
    "AvailabilityZone": "us-east-1d",
    "BackupRetentionPeriod": 7,
    "CaCertificateIdentifier": "certificate1",
    "CharacterSetName": "",
    "CopyTagsToSnapshot": true,
    "DbClusterIdentifier": "",
    "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",
    "DbInstanceClass": "db.t2.micro",
    "DbInstanceIdentifier": "database-1",
    "DbInstancePort": 0,
    "DbInstanceStatus": "available",
    "DbiResourceId": "db-EXAMPLE123",
    "DbName": "",
```

```
    "DbParameterGroups": [
        {
            "DbParameterGroupName": "default.mysql5.7",
            "ParameterApplyStatus": "in-sync"
        }
    ],
    "DbSecurityGroups": [],


    "DbSubnetGroup": {
        "DbSubnetGroupName": "my-group-123abc",
        "DbSubnetGroupDescription": "My subnet group",
        "VpcId": "vpc-example1",
        "SubnetGroupStatus": "Complete",
        "Subnets": [
            {
                "SubnetIdentifier": "subnet-123abc",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1d"
                },
                "SubnetStatus": "Active"
            },
            {
                "SubnetIdentifier": "subnet-456def",
                "SubnetAvailabilityZone": {
                    "Name": "us-east-1c"
                },
                "SubnetStatus": "Active"
            }
      ],
        "DbSubnetGroupArn": ""
    },
    "DeletionProtection": false,
    "DomainMemberships": [],
    "EnabledCloudWatchLogsExports": [],
    "Endpoint": {
        "address": "database-1.example.us-east-1.rds.amazonaws.com",
        "port": 3306,
        "hostedZoneId": "ZONEID1"
    },
    "Engine": "mysql",
    "EngineVersion": "5.7.22",
    "EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
```

```
    "IamDatabaseAuthenticationEnabled": false,
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "Iops": "",
    "KmsKeyId": "",
    "LatestRestorableTime": "2020-06-24T05:50:00.000Z",
    "LicenseModel": "general-public-license",
    "ListenerEndpoint": "",
    "MasterUsername": "admin",
    "MaxAllocatedStorage": 1000,
    "MonitoringInterval": 60,
    "MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
    "MultiAz": false,
    "OptionGroupMemberships": [
        {
            "OptionGroupName": "default:mysql-5-7",
            "Status": "in-sync"
        }
    ],
    "PreferredBackupWindow": "03:57-04:27",
    "PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
    "PendingModifiedValues": {
        "DbInstanceClass": "",
        "AllocatedStorage": "",
        "MasterUserPassword": "",
        "Port": "",
        "BackupRetentionPeriod": "",
        "MultiAZ": "",
        "EngineVersion": "",
        "LicenseModel": "",
        "Iops": "",
        "DbInstanceIdentifier": "",
        "StorageType": "",
        "CaCertificateIdentifier": "",
        "DbSubnetGroupName": "",
        "PendingCloudWatchLogsExports": "",
        "ProcessorFeatures": []
    },
    "PerformanceInsightsEnabled": false,
    "PerformanceInsightsKmsKeyId": "",
    "PerformanceInsightsRetentionPeriod": "",
    "ProcessorFeatures": [],
    "PromotionTier": "",
    "PubliclyAccessible": false,
    "ReadReplicaDBClusterIdentifiers": [],
```

```
    "ReadReplicaDBInstanceIdentifiers": [],
    "ReadReplicaSourceDBInstanceIdentifier": "",
    "SecondaryAvailabilityZone": "",
    "StatusInfos": [],
    "StorageEncrypted": false,
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
        {
            "VpcSecurityGroupId": "sg-example1",
            "Status": "active"
        }
    ]
}
```

AwsRdsDbSecurityGroup

Ob `AwsRdsDbSecurityGroup` jek berisi informasi tentang Layanan Database Relasional Amazon

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbSecurityGroup` objek. Untuk melihat deskripsi `AwsRdsDbSecurityGroup` atribut, lihat AwsRdsDbSecurityGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbSecurityGroup": {
    "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
    "DbSecurityGroupDescription": "default",
    "DbSecurityGroupName": "mysecgroup",
    "Ec2SecurityGroups": [
        {
          "Ec2SecurityGroupuId": "myec2group",
          "Ec2SecurityGroupName": "default",
          "Ec2SecurityGroupOwnerId": "987654321021",
          "Status": "authorizing"
        }
    ],
    "IpRanges": [
        {
          "Cidrip": "0.0.0.0/0",
          "Status": "authorizing"
        }
```

```
    ],
    "OwnerId": "123456789012",
    "VpcId": "vpc-1234567f"
}
```

AwsRdsDbSnapshot

Ob `AwsRdsDbSnapshot` jek berisi detail tentang snapshot cluster Amazon RDS DB.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsDbSnapshot` objek. Untuk melihat deskripsi `AwsRdsDbSnapshot` atribut, lihat AwsRdsDbSnapshotDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsDbSnapshot": {
    "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
    "DbInstanceIdentifier": "database-1",
    "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
    "Engine": "mysql",
    "AllocatedStorage": 20,
    "Status": "available",
    "Port": 3306,
    "AvailabilityZone": "us-east-1d",
    "VpcId": "vpc-example1",
    "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
    "MasterUsername": "admin",
    "EngineVersion": "5.7.22",
    "LicenseModel": "general-public-license",
    "SnapshotType": "automated",
    "Iops": null,
    "OptionGroupName": "default:mysql-5-7",
    "PercentProgress": 100,
    "SourceRegion": null,
    "SourceDbSnapshotIdentifier": "",
    "StorageType": "gp2",
    "TdeCredentialArn": "",
    "Encrypted": false,
    "KmsKeyId": "",
    "Timezone": "",
    "IamDatabaseAuthenticationEnabled": false,
    "ProcessorFeatures": [],
    "DbiResourceId": "db-resourceexample1"
```

```
}
```

AwsRdsEventSubscription

Ber `AwsRdsEventSubscription` isi detail tentang langganan notifikasi acara RDS. Langganan memungkinkan RDS untuk memposting acara ke topik SNS.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRdsEventSubscription` objek. Untuk melihat deskripsi `AwsRdsEventSubscription` atribut, lihat AwsRdsEventSubscriptionDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRdsEventSubscription": {
    "CustSubscriptionId": "myawsuser-secgrp",
    "CustomerAwsId": "111111111111",
    "Enabled": true,
    "EventCategoriesList": [
        "configuration change",
        "failure"
    ],
    "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
    "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
    "SourceIdsList": [
        "si-sample",
        "mysqldb-rr"
    ],
    "SourceType": "db-security-group",
    "Status": "creating",
    "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsRedshift` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsRedshiftCluster

Ob `AwsRedshiftCluster` jek berisi detail tentang cluster Amazon Redshift.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRedshiftCluster` objek. Untuk melihat deskripsi `AwsRedshiftCluster` atribut, lihat AwsRedshiftClusterDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRedshiftCluster": {
    "AllowVersionUpgrade": true,
    "AutomatedSnapshotRetentionPeriod": 1,
    "AvailabilityZone": "us-west-2d",
    "ClusterAvailabilityStatus": "Unavailable",
    "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
    "ClusterIdentifier": "redshift-cluster-1",
    "ClusterNodes": [
        {
            "NodeRole": "LEADER",
            "PrivateIPAddress": "192.0.2.108",
            "PublicIPAddress": "198.51.100.29"
        },
        {
            "NodeRole": "COMPUTE-0",
            "PrivateIPAddress": "192.0.2.22",
            "PublicIPAddress": "198.51.100.63"
        },
        {
             "NodeRole": "COMPUTE-1",
             "PrivateIPAddress": "192.0.2.224",
             "PublicIPAddress": "198.51.100.226"
        }
        ],
    "ClusterParameterGroups": [
        {
            "ClusterParameterStatusList": [
                {
                    "ParameterName": "max_concurrency_scaling_clusters",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "enable_user_activity_logging",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
```

```
                {
                    "ParameterName": "auto_analyze",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "query_group",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "datestyle",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "extra_float_digits",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "search_path",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "statement_timeout",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "wlm_json_configuration",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "require_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
                },
                {
                    "ParameterName": "use_fips_ssl",
                    "ParameterApplyStatus": "in-sync",
                    "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
```

```
                }
            ],
            "ParameterApplyStatus": "in-sync",
            "ParameterGroupName": "temp"
        }
    ],
    "ClusterPublicKey": "JalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
    "ClusterRevisionNumber": 17498,
    "ClusterSecurityGroups": [
        {
            "ClusterSecurityGroupName": "default",
            "Status": "active"
        }
    ],
    "ClusterSnapshotCopyStatus": {
        "DestinationRegion": "us-west-2",
        "ManualSnapshotRetentionPeriod": -1,
        "RetentionPeriod": 1,
        "SnapshotCopyGrantName": "snapshotCopyGrantName"
    },
    "ClusterStatus": "available",
    "ClusterSubnetGroupName": "default",
    "ClusterVersion": "1.0",
    "DBName": "dev",
    "DeferredMaintenanceWindows": [
        {
            "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
            "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
            "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
        }
     ],
    "ElasticIpStatus": {
        "ElasticIp": "203.0.113.29",
        "Status": "active"
    },
    "ElasticResizeNumberOfNodeOptions": "4",
    "Encrypted": false,
    "Endpoint": {
        "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
        "Port": 5439
    },
    "EnhancedVpcRouting": false,
    "ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
    "ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
```

```
    "HsmStatus": {
        "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
        "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
        "Status": "applying"
    },
    "IamRoles": [
        {
             "ApplyStatus": "in-sync",
             "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
        }
    ],
    "KmsKeyId": "kmsKeyId",
    "LoggingStatus": {
        "BucketName": "amzn-s3-demo-bucket",
        "LastFailureMessage": "test message",
        "LastFailureTime": "2020-08-09T13:00:00.000Z",
        "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
        "LoggingEnabled": true,
        "S3KeyPrefix": "/"
    },
    "MaintenanceTrackName": "current",
    "ManualSnapshotRetentionPeriod": -1,
    "MasterUsername": "awsuser",
    "NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
    "NodeType": "dc2.large",
    "NumberOfNodes": 2,
    "PendingActions": [],
    "PendingModifiedValues": {
        "AutomatedSnapshotRetentionPeriod": 0,
        "ClusterIdentifier": "clusterIdentifier",
        "ClusterType": "clusterType",
        "ClusterVersion": "clusterVersion",
        "EncryptionType": "None",
        "EnhancedVpcRouting": false,
        "MaintenanceTrackName": "maintenanceTrackName",
        "MasterUserPassword": "masterUserPassword",
        "NodeType": "dc2.large",
        "NumberOfNodes": 1,
        "PubliclyAccessible": true
    },
    "PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
    "PubliclyAccessible": true,
    "ResizeInfo": {
        "AllowCancelResize": true,
```

```
        "ResizeType": "ClassicResize"
    },
    "RestoreStatus": {
        "CurrentRestoreRateInMegaBytesPerSecond": 15,
        "ElapsedTimeInSeconds": 120,
        "EstimatedTimeToCompletionInSeconds": 100,
        "ProgressInMegaBytes": 10,
        "SnapshotSizeInMegaBytes": 1500,
        "Status": "restoring"
    },
    "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
    "SnapshotScheduleState": "ACTIVE",
     "VpcId": "vpc-example",
    "VpcSecurityGroups": [
        {
            "Status": "active",
            "VpcSecurityGroupId": "sg-example"
        }
    ]
}
```

AwsRoute53 sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsRoute53` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsRoute53HostedZone

Ob `AwsRoute53HostedZone` jek menyediakan informasi tentang zona yang dihosting Amazon Route 53, termasuk empat server nama yang ditugaskan ke zona yang dihosting. Zona yang dihosting mewakili kumpulan catatan yang dapat dikelola bersama, milik nama domain induk tunggal.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsRoute53HostedZone` objek. Untuk melihat deskripsi `AwsRoute53HostedZone` atribut, lihat AwsRoute53HostedZoneDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsRoute53HostedZone": {
```

```
    "HostedZone": {
        "Id": "Z06419652JEMGO9TA2XKL",
        "Name": "asff.testing",
        "Config": {
            "Comment": "This is an example comment."
        }
    },
    "NameServers": [
        "ns-470.awsdns-32.net",
        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}
```

AWSS3 sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsS3` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsS3AccessPoint

`AwsS3AccessPoint`menyediakan informasi tentang titik akses Amazon S3. Titik akses S3 diberi nama titik akhir jaringan yang dilampirkan ke bucket S3 yang dapat Anda gunakan untuk melakukan operasi objek S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3AccessPoint` objek. Untuk melihat deskripsi `AwsS3AccessPoint` atribut, lihat AwsS3AccessPointDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsS3AccessPoint": {
        "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
        "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
        "Bucket": "amzn-s3-demo-bucket",
        "BucketAccountId": "123456789012",
        "Name": "asff-access-point",
        "NetworkOrigin": "VPC",
        "PublicAccessBlockConfiguration": {
            "BlockPublicAcls": true,
            "BlockPublicPolicy": true,
            "IgnorePublicAcls": true,
            "RestrictPublicBuckets": true
        },
        "VpcConfiguration": {
            "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
        }
}
```

AwsS3AccountPublicAccessBlock

`AwsS3AccountPublicAccessBlock`menyediakan informasi tentang konfigurasi Blok Akses Publik Amazon S3 untuk akun.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3AccountPublicAccessBlock` objek. Untuk melihat deskripsi `AwsS3AccountPublicAccessBlock` atribut, lihat AwsS3AccountPublicAccessBlockDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
```

```
}
```

AWSS3Bucket

Ob `AwsS3Bucket` jek memberikan detail tentang bucket Amazon S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3Bucket` objek. Untuk melihat deskripsi `AwsS3Bucket` atribut, lihat AwsS3BucketDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsS3Bucket": {
    "AccessControlList": "{\"grantSet\":null,\"grantList\":[{\"grantee\":{\"id\":
\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\",\"displayName
\":null},\"permission\":\"FullControl\"},{\"grantee\":\"AllUsers\",\"permission\":
\"ReadAcp\"},{\"grantee\":\"AuthenticatedUsers\",\"permission\":\"ReadAcp\"}",,
    "BucketLifecycleConfiguration": {
       "Rules": [
           {
               "AbortIncompleteMultipartUpload": {
                   "DaysAfterInitiation": 5
               },
               "ExpirationDate": "2021-11-10T00:00:00.000Z",
               "ExpirationInDays": 365,
               "ExpiredObjectDeleteMarker": false,
               "Filter": {
                   "Predicate": {
                       "Operands": [
                           {
                               "Prefix": "tmp/",
                               "Type": "LifecyclePrefixPredicate"
                           },
                           {
                               "Tag": {
                                   "Key": "ArchiveAge",
                                   "Value": "9m"
                               },
                               "Type": "LifecycleTagPredicate"
                           }
                       ],
                       "Type": "LifecycleAndOperator"
                   }
```

```
            },
            "ID": "Move rotated logs to Glacier",
            "NoncurrentVersionExpirationInDays": -1,
            "NoncurrentVersionTransitions": [
                {
                    "Days": 2,
                    "StorageClass": "GLACIER"
                }
            ],
            "Prefix": "rotated/",
            "Status": "Enabled",
            "Transitions": [
                {
                    "Date": "2020-11-10T00:00:00.000Z",
                    "Days": 100,
                    "StorageClass": "GLACIER"
                }
            ]
        }
    ]
},
"BucketLoggingConfiguration": {
 "DestinationBucketName": "s3serversideloggingbucket-123456789012",
 "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "amzn-s3-demo-bucket",
"BucketNotificationConfiguration": {
 "Configurations": [{
  "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
  "Events": [
   "s3:ObjectCreated:Put"
  ],
  "Filter": {
   "S3KeyFilter": {
    "FilterRules": [
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
     "Value": "pre"
    },
    {
     "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
     "Value": "suf"
    },
    ]
```

```
        }
       },
       "Type": "LambdaConfiguration"
      }]
     },
     "BucketVersioningConfiguration": {
      "IsMfaDeleteEnabled": true,
      "Status": "Off"
     },
     "BucketWebsiteConfiguration": {
      "ErrorDocument": "error.html",
      "IndexDocumentSuffix": "index.html",
      "RedirectAllRequestsTo": {
       "HostName": "example.com",
       "Protocol": "http"
      },
      "RoutingRules": [{
       "Condition": {
        "HttpErrorCodeReturnedEquals": "Redirected",
        "KeyPrefixEquals": "index"
          },
       "Redirect": {
        "HostName": "example.com",
        "HttpRedirectCode": "401",
        "Protocol": "HTTP",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
       }
      }]
     },
     "CreatedAt": "2007-11-30T01:46:56.000Z",
     "ObjectLockConfiguration": {
      "ObjectLockEnabled": "Enabled",
      "Rule": {
       "DefaultRetention": {
        "Days": null,
        "Mode": "GOVERNANCE",
        "Years": 12
       },
      },
     },
     "OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
     "OwnerName": "s3bucketowner",
     "PublicAccessBlockConfiguration": {
```

```
        "BlockPublicAcls": true,
        "BlockPublicPolicy": true,
        "IgnorePublicAcls": true,
        "RestrictPublicBuckets": true,
    },
    "ServerSideEncryptionConfiguration": {
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "AES256",
                    "KMSMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
                }
            }
        ]
     }
}
```

AWSS3Objek

Ob `AwsS3Object` jek menyediakan informasi tentang objek Amazon S3.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsS3Object` objek. Untuk melihat deskripsi `AwsS3Object` atribut, lihat AwsS3ObjectDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsS3Object": {
    "ContentType": "text/html",
    "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
    "LastModified": "2012-04-23T18:25:43.511Z",
    "ServerSideEncryption": "aws:kms",
    "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-
a9a0-608ec069e5a7",
    "VersionId": "ws31OurgOOjH_HHllIxPE35P.MELYaYh"
}
```

AwsSageMaker sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsSageMaker` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsSageMakerNotebookInstance

Ob `AwsSageMakerNotebookInstance` jek menyediakan informasi tentang instance notebook Amazon SageMaker AI, yang merupakan instance komputasi pembelajaran mesin yang menjalankan Aplikasi Notebook Jupyter.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSageMakerNotebookInstance` objek. Untuk melihat deskripsi `AwsSageMakerNotebookInstance` atribut, lihat AwsSageMakerNotebookInstanceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsSageMakerNotebookInstance": {
    "DirectInternetAccess": "Disabled",
    "InstanceMetadataServiceConfiguration": {
     "MinimumInstanceMetadataServiceVersion": "1",
    },
    "InstanceType": "ml.t2.medium",
    "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
    "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
    "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/
sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
    "NotebookInstanceName":
 "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
    "NotebookInstanceStatus": "InService",
    "PlatformIdentifier": "notebook-al1-v1",
    "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-
SageMakerCustomExecution-1R0X32HGC38IW",
    "RootAccess": "Disabled",
    "SecurityGroups": [
     "sg-06b347359ab068745"
    ],
    "SubnetId": "subnet-02c0deea5fa64578e",
    "Url":
 "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-
east-1.sagemaker.aws",
    "VolumeSizeInGB": 5
}
```

AwsSecretsManager sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsSecretsManager` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsSecretsManagerSecret

Ob `AwsSecretsManagerSecret` jek memberikan rincian tentang rahasia Manajer Rahasia.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSecretsManagerSecret` objek. Untuk melihat deskripsi `AwsSecretsManagerSecret` atribut, lihat AwsSecretsManagerSecretDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsSecretsManagerSecret": {
    "RotationRules": {
        "AutomaticallyAfterDays": 30
    },
    "RotationOccurredWithinFrequency": true,
    "KmsKeyId": "kmsKeyId",
    "RotationEnabled": true,
    "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
    "Deleted": false,
    "Name": "MyTestDatabaseSecret",
    "Description": "My test database secret"
}
```

AwsSns sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsSns` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsSnsTopic

Ob `AwsSnsTopic` jek berisi detail tentang topik Layanan Pemberitahuan Sederhana Amazon.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSnsTopic` objek. Untuk melihat deskripsi `AwsSnsTopic` atribut, lihat AwsSnsTopicDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
    "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
    "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
    "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
    "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
    "KmsMasterKeyId": "alias/ExampleAlias",
    "Owner": "123456789012",
    "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",
    "SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsSuccessFeedbackRoleArn",
    "Subscription": {
         "Endpoint": "http://sampleendpoint.com",
         "Protocol": "http"
    },
    "TopicName": "SampleTopic"
}
```

AwsSqs sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsSqs` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsSqsQueue

Ob `AwsSqsQueue` jek berisi informasi tentang antrian Amazon Simple Queue Service.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSqsQueue` objek. Untuk melihat deskripsi `AwsSqsQueue` atribut, lihat AwsSqsQueueDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsSsm` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsSsmPatchCompliance

Ob `AwsSsmPatchCompliance` jek memberikan informasi tentang status patch pada instance berdasarkan baseline patch yang digunakan untuk menambal instance.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsSsmPatchCompliance` objek. Untuk melihat deskripsi `AwsSsmPatchCompliance` atribut, lihat AwsSsmPatchComplianceDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsSsmPatchCompliance": {
    "Patch": {
        "ComplianceSummary": {
            "ComplianceType": "Patch",
            "CompliantCriticalCount": 0,
            "CompliantHighCount": 0,
            "CompliantInformationalCount": 0,
            "CompliantLowCount": 0,
            "CompliantMediumCount": 0,
            "CompliantUnspecifiedCount": 461,
```

```
            "ExecutionType": "Command",
            "NonCompliantCriticalCount": 0,
            "NonCompliantHighCount": 0,
            "NonCompliantInformationalCount": 0,
            "NonCompliantLowCount": 0,
            "NonCompliantMediumCount": 0,
            "NonCompliantUnspecifiedCount": 0,
            "OverallSeverity": "UNSPECIFIED",
            "PatchBaselineId": "pb-0c5b2769ef7cbe587",
            "PatchGroup": "ExamplePatchGroup",
            "Status": "COMPLIANT"
        }
    }
}
```

AwsStepFunctions sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsStepFunctions` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsStepFunctionStateMachine

Ob `AwsStepFunctionStateMachine` jek menyediakan informasi tentang mesin AWS Step Functions status, yang merupakan alur kerja yang terdiri dari serangkaian langkah yang digerakkan oleh peristiwa.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsStepFunctionStateMachine` objek. Untuk melihat deskripsi `AwsStepFunctionStateMachine` atribut, lihat AwsStepFunctionStateMachine di Referensi AWS Security Hub API.

Contoh

```
"AwsStepFunctionStateMachine": {
    "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
    "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
    "Status": "ACTIVE",
```

```
    "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RVO1UKT",
    "Type": "STANDARD",
    "LoggingConfiguration": {
        "Level": "OFF",
        "IncludeExecutionData": false
    },
    "TracingConfiguration": {
        "Enabled": false
    }
}
```

AwsWaf sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsWaf` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

AwsWafRateBasedRule

Ob `AwsWafRateBasedRule` jek berisi detail tentang aturan AWS WAF berbasis tarif untuk sumber daya global. A AWS WAF turan berbasis tarif menyediakan pengaturan untuk menunjukkan kapan harus mengizinkan, memblokir, atau menghitung permintaan. Rate-based aturan mencakup jumlah permintaan yang tiba selama periode waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRateBasedRule` objek. Untuk melihat deskripsi `AwsWafRateBasedRule` atribut, lihat AwsWafRateBasedRuleDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
```

```
}
```

AwsWafRegionalRateBasedRule

Ob `AwsWafRegionalRateBasedRule` jek berisi detail tentang aturan berbasis tarif untuk sumber daya Regional. Aturan berbasis tarif menyediakan pengaturan untuk menunjukkan kapan harus mengizinkan, memblokir, atau menghitung permintaan. Rate-based aturan mencakup jumlah permintaan yang tiba selama periode waktu tertentu.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRateBasedRule` objek. Untuk melihat deskripsi `AwsWafRegionalRateBasedRule` atribut, lihat AwsWafRegionalRateBasedRuleDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRateBasedRule":{
    "MatchPredicates" : [{
        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    }],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}
```

AwsWafRegionalRule

Ob `AwsWafRegionalRule` jek memberikan rincian tentang aturan AWS WAF Regional. Aturan ini mengidentifikasi permintaan web yang ingin Anda izinkan, blokir, atau hitung.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRule` objek. Untuk melihat deskripsi `AwsWafRegionalRule` atribut, lihat AwsWafRegionalRuleDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRule": {
```

```
    "MetricName": "SampleWAF_Rule__Metric_1",
    "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
    "PredicateList": [{
        "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
        "Negated": false,
        "Type": "GeoMatch"
    }]
}
```

AwsWafRegionalRuleGroup

Ob `AwsWafRegionalRuleGroup` jek memberikan rincian tentang grup aturan AWS WAF Regional. Grup aturan adalah kumpulan aturan yang telah ditentukan sebelumnya yang Anda tambahkan ke daftar kontrol akses web (ACL web).

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafRegionalRuleGroup` objek. Untuk melihat deskripsi `AwsWafRegionalRuleGroup` atribut, lihat AwsWafRegionalRuleGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW"
        }
    }],
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl`memberikan rincian tentang daftar kontrol akses web AWS WAF Regional (ACL web). ACL web berisi aturan yang mengidentifikasi permintaan yang ingin Anda izinkan, blokir, atau hitung.

Berikut ini adalah contoh `AwsWafRegionalWebAcl` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsWafRegionalWebAclDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRegionalWebAcl": {
    "DefaultAction": "ALLOW",
    "MetricName" : "web-regional-webacl-metric-1",
    "Name": "WebACL_123",
    "RulesList": [
        {
            "Action": {
                "Type": "Block"
            },
            "Priority": 3,
            "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
            "Type": "REGULAR",
            "ExcludedRules": [
                {
                    "ExclusionType": "Exclusion",
                    "RuleId": "Rule_id_1"
                }
            ],
            "OverrideAction": {
                "Type": "OVERRIDE"
            }
        }
    ],
    "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule`memberikan informasi tentang AWS WAF aturan. A AWS WAF turan mengidentifikasi permintaan web yang ingin Anda izinkan, blokir, atau hitung.

Berikut ini adalah contoh `AwsWafRule` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsWafRuleDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRule": {
    "MetricName": "AwsWafRule_Metric_1",
    "Name": "AwsWafRule_Name_1",
    "PredicateList": [{
        "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
        "Negated": false,
        "Type": "GeoMatch"
    }],
    "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup`memberikan informasi tentang grup AWS WAF aturan. Grup AWS WAF aturan adalah kumpulan aturan yang telah ditentukan sebelumnya yang Anda tambahkan ke daftar kontrol akses web (ACL web).

Berikut ini adalah contoh `AwsWafRuleGroup` penemuan dalam AWS Security Finding Format (ASFF). Untuk melihat deskripsi `AwsApiGatewayV2Stage` atribut, lihat AwsWafRuleGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafRuleGroup": {
    "MetricName": "SampleWAF_Metric_1",
    "Name": "bb-WAFRuleGroupWithRuleCompliant",
    "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
    "Rules": [{
        "Action": {
            "Type": "ALLOW",
        },
        "Priority": 1,
        "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
        "Type": "REGULAR"
    }]
}
```

AwsWafv2RuleGroup

Ob `AwsWafv2RuleGroup` jek memberikan rincian tentang grup aturan AWS WAF V2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafv2RuleGroup` objek. Untuk melihat deskripsi `AwsWafv2RuleGroup` atribut, lihat AwsWafv2RuleGroupDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafv2RuleGroup": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1000,
    "Description": "Resource for ASFF",
    "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Name": "wafv2rulegroupasff",
    "Rules": [{
     "Action": {
     "Allow": {
      "CustomRequestHandling": {
       "InsertHeaders": [
        {
        "Name": "AllowActionHeader1Name",
        "Value": "AllowActionHeader1Value"
        },
        {
        "Name": "AllowActionHeader2Name",
        "Value": "AllowActionHeader2Value"
        }
       ]
      }
     },
     "Name": "RuleOne",
     "Priority": 1,
     "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,
      "MetricName": "rulegroupasff",
      "SampledRequestsEnabled": false
     }
    }],
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "rulegroupasff",
     "SampledRequestsEnabled": false
    }
}
```

AwsWafWebAcl

Ob `AwsWafWebAcl` jek memberikan rincian tentang ACL AWS WAF web.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafWebAcl` objek. Untuk melihat deskripsi `AwsWafWebAcl` atribut, lihat AwsWafWebAclDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafWebAcl": {
    "DefaultAction": "ALLOW",
    "Name": "MyWafAcl",
    "Rules": [
        {
            "Action": {
                "Type": "ALLOW"
            },
            "ExcludedRules": [
                {
                    "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
                }
            ],
            "OverrideAction": {
                "Type": "NONE"
            },
            "Priority": 1,
            "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
            "Type": "REGULAR"
        }
    ],
    "WebAclId": "waf-1234567890"
}
```

AwsWafv2WebAcl

Ob `AwsWafv2WebAcl` jek memberikan rincian tentang ACL web AWS WAF V2.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsWafv2WebAcl` objek. Untuk melihat deskripsi `AwsWafv2WebAcl` atribut, lihat AwsWafv2WebAclDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsWafv2WebAcl": {
    "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Capacity": 1326,
    "CaptchaConfig": {
     "ImmunityTimeProperty": {
      "ImmunityTime": 500
     }
    },
    "DefaultAction": {
     "Block": {}
    },
    "Description": "Web ACL for JsonBody testing",
    "ManagedbyFirewallManager": false,
    "Name": "WebACL-RoaD4QexqSxG",
    "Rules": [{
     "Action": {
      "RuleAction": {
       "Block": {}
      }
     },
     "Name": "TestJsonBodyRule",
     "Priority": 1,
     "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
     }
    }],
    "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestingJsonBodyMetric"
    }
}
```


AwsXray sumber daya dalam ASFF

Berikut ini adalah contoh sintaks AWS Security Finding Format (ASFF) untuk `AwsXray` sumber daya.

AWS Security Hub CSPM menormalkan temuan dari berbagai sumber ke dalam ASFF. Untuk informasi latar belakang tentang ASFF, lihat[AWS Format Penemuan Keamanan (ASFF)](#).

AwsXrayEncryptionConfig

Ob `AwsXrayEncryptionConfig` jek berisi informasi tentang konfigurasi enkripsi untuk AWS X-Ray.

Contoh berikut menunjukkan AWS Security Finding Format (ASFF) untuk `AwsXrayEncryptionConfig` objek. Untuk melihat deskripsi `AwsXrayEncryptionConfig` atribut, lihat AwsXrayEncryptionConfigDetails di Referensi AWS Security Hub API.

Contoh

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

CodeRepository objek dalam ASFF

Ob `CodeRepository` jek menyediakan informasi tentang repositori kode eksternal yang Anda sambungkan ke AWS sumber daya dan mengonfigurasi Amazon Inspector untuk memindai kerentanan.

Contoh berikut menunjukkan sintaks AWS Security Finding Format (ASFF) untuk `CodeRepository` objek. Untuk melihat deskripsi `CodeRepository` atribut, lihat CodeRepositoryDetails di Referensi AWS Security Hub API. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

Contoh

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

Kontainer objek dalam ASFF

Contoh berikut menunjukkan sintaks AWS Security Finding Format (ASFF) untuk `Container` objek. Untuk melihat deskripsi `Container` atribut, lihat ContainerDetails di Referensi AWS Security Hub API. Untuk informasi latar belakang tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

Contoh

```
"Container": {
    "ContainerRuntime": "docker",
    "ImageId": "image12",
    "ImageName": "1111111/
knotejs@sha256:372131c9fef111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "Name": "knote",
    "Privileged": true,
    "VolumeMounts": [{
        "Name": "vol-03909e9",
        "MountPath": "/mnt/etc"
    }]
}
```

Lainnya objek dalam ASFF

Dalam Format AWS Penemuan Keamanan (ASFF), `Other` objek menentukan bidang dan nilai kustom. Untuk informasi lebih lanjut tentang ASFF, lihatAWS Format Penemuan Keamanan (ASFF).

Dengan menggunakan `Other` objek, Anda dapat menentukan bidang dan nilai kustom untuk sumber daya. Anda dapat menggunakan `Other` objek untuk kasus berikut:

- Jenis sumber daya tidak memiliki `Details` objek yang sesuai. Untuk menentukan detail sumber daya, gunakan `Other` objek.
- Ob `Details` jek untuk jenis sumber daya tidak menyertakan semua atribut yang ingin Anda tentukan. Dalam hal ini, gunakan `Details` objek untuk jenis sumber daya untuk menentukan atribut yang tersedia. Gunakan `Other` objek untuk menentukan atribut yang tidak ada dalam `Details` objek tipe spesifik.
- Jenis sumber daya bukan salah satu jenis yang disediakan. Dalam hal ini, atur `Resource.Type` ke `Other` dan gunakan `Other` objek untuk menentukan detailnya.

Jenis: Peta hingga 50 pasangan kunci-nilai

Setiap pasangan kunci-nilai harus memenuhi persyaratan berikut.

- Kunci harus berisi kurang dari 128 karakter.
- Nilai harus berisi kurang dari 1.024 karakter.

Melihat wawasan di Security Hub CSPM

Di AWS Security Hub CSPM, wawasan adalah kumpulan temuan terkait. Wawasan dapat mengidentifikasi area keamanan tertentu yang membutuhkan perhatian dan intervensi. Misalnya, wawasan mungkin menunjukkan instans EC2 yang merupakan subjek temuan yang mendeteksi praktik keamanan yang buruk. Wawasan menyatukan temuan dari seluruh penyedia pencarian.

Setiap wawasan didefinisikan oleh grup berdasarkan pernyataan dan filter opsional. Kelompok berdasarkan pernyataan menunjukkan bagaimana mengelompokkan temuan yang cocok, dan mengidentifikasi jenis item yang diterapkan wawasan tersebut. Misalnya, jika wawasan dikelompokkan berdasarkan pengidentifikasi sumber daya, maka wawasan menghasilkan daftar pengidentifikasi sumber daya. Filter opsional mengidentifikasi temuan yang cocok untuk wawasan. Misalnya, Anda mungkin ingin hanya melihat temuan dari penyedia atau temuan tertentu yang terkait dengan jenis sumber daya tertentu.

Security Hub CSPM menawarkan beberapa wawasan terkelola bawaan. Anda tidak dapat mengubah atau menghapus wawasan terkelola. Untuk melacak masalah keamanan yang unik untuk AWS lingkungan dan penggunaan Anda, Anda dapat membuat wawasan khusus.

Halaman Wawasan di konsol CSPM AWS Security Hub menampilkan daftar wawasan yang tersedia.

Secara default, daftar menampilkan wawasan terkelola dan kustom. Untuk memfilter daftar wawasan berdasarkan jenis wawasan, pilih jenis wawasan dari menu tarik-turun yang berada di sebelah bidang filter.

- Untuk menampilkan semua wawasan yang tersedia, pilih Semua wawasan. Ini adalah pilihan default.
- Untuk hanya menampilkan wawasan terkelola, pilih wawasan terkelola CSPM Security Hub.
- Untuk hanya menampilkan wawasan khusus, pilih Wawasan khusus.

Anda juga dapat memfilter daftar wawasan berdasarkan nama wawasan. Untuk melakukannya, di bidang filter, ketikkan teks yang akan digunakan untuk memfilter daftar. Filter tidak peka huruf besar/kecil. Filter mencari wawasan yang berisi teks di mana saja dalam nama wawasan.

Wawasan hanya mengembalikan hasil jika Anda telah mengaktifkan integrasi atau standar yang menghasilkan temuan yang cocok. Misalnya, wawasan terkelola 29. Sumber daya teratas berdasarkan jumlah pemeriksaan CIS yang gagal hanya mengembalikan hasil jika Anda mengaktifkan versi standar Benchmark Yayasan Center for Internet Security (CISAWS).

Meninjau dan bertindak berdasarkan wawasan di Security Hub CSPM

Untuk setiap wawasan, AWS Security Hub CSPM pertama-tama menentukan temuan yang cocok dengan kriteria filter, dan kemudian menggunakan atribut pengelompokan untuk mengelompokkan temuan yang cocok.

Dari halaman Wawasan di konsol, Anda dapat melihat dan mengambil tindakan pada hasil dan temuan.

Jika Anda mengaktifkan agregasi lintas wilayah, hasil untuk wawasan terkelola (saat Anda masuk ke Wilayah agregasi) menyertakan temuan dari Wilayah agregasi dan Wilayah tertaut. Hasil untuk wawasan kustom, jika wawasan tidak difilter berdasarkan Wilayah, juga menyertakan temuan dari Wilayah agregasi dan Wilayah tertaut (saat Anda masuk ke Wilayah agregasi). Di Wilayah lain, hasil wawasan hanya untuk Wilayah tersebut.

Untuk informasi tentang mengkonfigurasi agregasi lintas wilayah, lihatthe section called “Menggabungkan data di seluruh Wilayah”.

Melihat dan mengambil tindakan pada hasil wawasan

Hasil wawasan terdiri dari daftar hasil yang dikelompokkan untuk wawasan. Misalnya, jika wawasan dikelompokkan berdasarkan pengidentifikasi sumber daya, maka hasil wawasan adalah daftar pengidentifikasi sumber daya. Setiap item dalam daftar hasil menunjukkan jumlah temuan yang cocok untuk item tersebut.

Jika temuan dikelompokkan berdasarkan pengidentifikasi sumber daya atau jenis sumber daya, hasilnya mencakup semua sumber daya dalam temuan yang cocok. Ini termasuk sumber daya yang memiliki tipe berbeda dari jenis sumber daya yang ditentukan dalam kriteria filter. Misalnya, wawasan mengidentifikasi temuan yang terkait dengan bucket S3. Jika temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM, hasil wawasan menyertakan kedua sumber daya.

Pada konsol CSPM Security Hub, daftar hasil diurutkan dari temuan yang paling cocok hingga paling sedikit. Security Hub CSPM hanya dapat menampilkan 100 hasil. Jika ada lebih dari 100 nilai pengelompokan, Anda hanya melihat 100 pertama.

Selain daftar hasil, hasil wawasan menampilkan serangkaian grafik yang merangkum jumlah temuan yang cocok untuk atribut berikut.

- Label keparahan — Jumlah temuan untuk setiap label keparahan
- Akun AWS ID — Lima ID akun teratas untuk temuan yang cocok

- Jenis sumber daya - Lima jenis sumber daya teratas untuk temuan yang cocok
- ID Sumber Daya — Lima ID sumber daya teratas untuk temuan yang cocok
- Nama produk - Lima penyedia pencarian teratas untuk temuan yang cocok

Jika Anda telah mengonfigurasi tindakan kustom, maka Anda dapat mengirim hasil yang dipilih ke tindakan kustom. Tindakan harus dikaitkan dengan CloudWatch aturan Amazon untuk jenis `Security Hub Insight Results` acara. Untuk informasi selengkapnya, lihat the section called "Respon dan remediasi otomatis". Jika Anda belum mengonfigurasi tindakan kustom, menu T indakan dinonaktifkan.

Security Hub CSPM console

Untuk melihat dan mengambil tindakan pada hasil wawasan (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, silakan pilih Wawasan.
3. Untuk menampilkan daftar hasil wawasan, pilih nama wawasan.
4. Pilih kotak centang untuk setiap hasil yang akan dikirim ke tindakan kustom.
5. Dari menu Tindakan, pilih tindakan kustom.

Security Hub CSPM API, AWS CLI

Untuk melihat dan mengambil tindakan pada hasil wawasan (API, AWS CLI)

Untuk melihat hasil wawasan, gunakan pen >GetInsightResults goperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan get-insight-results perintah.

Untuk mengidentifikasi wawasan untuk mengembalikan hasilnya, Anda memerlukan wawasan ARN. Untuk mendapatkan ARN wawasan untuk wawasan khusus, gunakan operasi `GetInsights` API atau get-insight-results perintah.

Contoh berikut mengambil hasil untuk wawasan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

Untuk informasi tentang cara membuat tindakan kustom secara terprogram, lihat. Menggunakan tindakan khusus untuk mengirim hasil temuan dan wawasan ke EventBridge

Melihat dan mengambil tindakan pada temuan hasil wawasan (konsol)

Dari daftar hasil wawasan di konsol CSPM Security Hub, Anda dapat menampilkan daftar temuan untuk setiap hasil.

Untuk menampilkan dan mengambil tindakan pada temuan wawasan (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, silakan pilih Wawasan.
3. Untuk menampilkan daftar hasil wawasan, pilih nama wawasan.
4. Untuk menampilkan daftar temuan untuk hasil wawasan, pilih item dari daftar hasil. Daftar temuan menunjukkan temuan aktif untuk hasil wawasan yang dipilih yang memiliki status alur kerja `NEW` atau`NOTIFIED`.

Dari daftar temuan, Anda dapat melakukan tindakan berikut:

- Penyaringan temuan di Security Hub CSPM
- Meninjau detail dan sejarah temuan
- Mengatur status alur kerja temuan di Security Hub CSPM
- Mengirim temuan ke tindakan CSPM Hub Keamanan kustom

Wawasan terkelola di Security Hub CSPM

AWSSecurity Hub CSPM memberikan beberapa wawasan terkelola.

Anda tidak dapat mengedit atau menghapus wawasan terkelola CSPM Security Hub. Anda dapat melihat dan mengambil tindakan atas hasil dan temuan wawasan. Anda juga dapat menggunakan wawasan terkelola sebagai dasar untuk wawasan kustom baru.

Seperti semua wawasan, wawasan terkelola hanya mengembalikan hasil jika Anda telah mengaktifkan integrasi produk atau standar keamanan yang dapat menghasilkan temuan yang cocok.

Untuk wawasan yang dikelompokkan berdasarkan pengenal sumber daya, hasilnya mencakup pengidentifikasi semua sumber daya dalam temuan yang cocok. Ini termasuk sumber daya yang memiliki tipe berbeda dari jenis sumber daya dalam kriteria filter. Misalnya, wawasan 2 dalam daftar berikut mengidentifikasi temuan yang terkait dengan bucket Amazon S3. Jika temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM, hasil wawasan menyertakan kedua sumber daya tersebut.

Security Hub CSPM saat ini menawarkan wawasan terkelola berikut:

1. AWSsumber daya dengan temuan terbanyak

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   Dikelompokkan berdasarkan: Pengenal sumber daya

   Menemukan filter:

   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

2. Bucket S3 dengan izin tulis atau baca publik

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   Dikelompokkan berdasarkan: Pengenal sumber daya

   Menemukan filter:

   - Jenis dimulai dengan `Effects/Data Exposure`
   - Jenis sumber daya adalah `AwsS3Bucket`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

3. AMI yang menghasilkan temuan terbanyak

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   Dikelompokkan berdasarkan: ID gambar instans EC2

   Menemukan filter:

   - Jenis sumber daya adalah `AwsEc2Instance`
   - Record state adalah `ACTIVE`

- Status alur kerja adalah `NEW` atau `NOTIFIED`

4. Contoh EC2 yang terlibat dalam Taktik, Teknik, dan Prosedur (TTP) yang dikenal

   ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

   Dikelompokkan berdasarkan: Resource ID

   Menemukan filter:

   - Jenis dimulai dengan `TTPs`
   - Jenis sumber daya adalah `AwsEc2Instance`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

5. AWSkepala sekolah dengan aktivitas kunci akses yang mencurigakan

   ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

   Dikelompokkan berdasarkan: Nama utama kunci akses IAM

   Menemukan filter:

   - Jenis sumber daya adalah `AwsIamAccessKey`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

6. AWScontoh sumber daya yang tidak memenuhi standar keamanan/praktik terbaik

   ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

   Dikelompokkan berdasarkan: Resource ID

   Menemukan filter:

   - Tipe adalah `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

7. AWSsumber daya yang terkait dengan eksfiltrasi data potensial

   ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

   Dikelompokkan berdasarkan:: Resource ID

Menemukan filter:

- Jenis dimulai dengan Effects/Data Eksfiltrasi/
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

8. AWSsumber daya yang terkait dengan konsumsi sumber daya yang tidak sah

   ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

   Dikelompokkan berdasarkan: Resource ID

   Menemukan filter:

   - Jenis dimulai dengan `Effects/Resource Consumption`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

9. Bucket S3 yang tidak memenuhi standar keamanan/praktik terbaik

   ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

   Dikelompokkan berdasarkan: Resource ID

   Menemukan filter:

   - Jenis sumber daya adalah `AwsS3Bucket`
   - Tipe adalah `Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices`
   - Record state adalah `ACTIVE`
   - Status alur kerja adalah `NEW` atau `NOTIFIED`

10. Bucket S3 dengan data sensitif

    ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis sumber daya adalah `AwsS3Bucket`
    - Jenis dimulai dengan `Sensitive Data Identifications/`
    - Record state adalah `ACTIVE`

- Status alur kerja adalah `NEW` atau `NOTIFIED`

11. Kredensi yang mungkin bocor

    ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis dimulai dengan `Sensitive Data Identifications/Passwords/`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

12. Instans EC2 yang memiliki patch keamanan yang hilang untuk kerentanan penting

    ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis dimulai dengan `Software and Configuration Checks/Vulnerabilities/CVE`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

13. Instans EC2 dengan perilaku umum yang tidak biasa

    ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis dimulai dengan `Unusual Behaviors`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

14. Instans EC2 yang memiliki port yang dapat diakses dari Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- Jenis dimulai dengan `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
- Jenis sumber daya adalah `AwsEc2Instance`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

15. Instans EC2 yang tidak memenuhi standar keamanan/praktik terbaik

    ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis dimulai dengan salah satu dari berikut ini:
      - `Software and Configuration Checks/Industry and Regulatory Standards/`
      - `Software and Configuration Checks/AWSSecurity Best Practices`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

16. Instans EC2 yang terbuka untuk Internet

    ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis dimulai dengan `Software and Configuration Checks/AWS Security Best Practices/Network Reachability`
    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

17. Instans EC2 yang terkait dengan pengintaian musuh

    ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- Tipe dimulai dengan TTPs/Discovery/Recon
- Jenis sumber daya adalah `AwsEc2Instance`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

18. AWSsumber daya yang terkait dengan malware

ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- Jenis dimulai dengan salah satu dari berikut ini:
  - `Effects/Data Exfiltration/Trojan`
  - `TTPs/Initial Access/Trojan`
  - `TTPs/Command and Control/Backdoor`
  - `TTPs/Command and Control/Trojan`
  - `Software and Configuration Checks/Backdoor`
  - `Unusual Behaviors/VM/Backdoor`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

19. AWSsumber daya yang terkait dengan masalah cryptocurrency

ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- Jenis dimulai dengan salah satu dari berikut ini:
  - `Effects/Resource Consumption/Cryptocurrency`
  - `TTPs/Command and Control/CryptoCurrency`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

20. AWSsumber daya dengan upaya akses yang tidak sah

    ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis dimulai dengan salah satu dari berikut ini:
      - `TTPs/Command and Control/UnauthorizedAccess`
      - `TTPs/Initial Access/UnauthorizedAccess`
      - `Effects/Data Exfiltration/UnauthorizedAccess`
      - `Unusual Behaviors/User/UnauthorizedAccess`
      - `Effects/Resource Consumption/UnauthorizedAccess`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
21. Indikator Ancaman Intel dengan hit terbanyak dalam seminggu terakhir

    ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

    Menemukan filter:

    - Dibuat dalam 7 hari terakhir
22. Akun teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

    Dikelompokkan berdasarkan: ID Akun AWS

    Menemukan filter:

    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`
23. Produk teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

    Dikelompokkan berdasarkan: Nama produk

    Menemukan filter:

    - Record state adalah `ACTIVE`

- Status alur kerja adalah `NEW` atau `NOTIFIED`

24. Keparahan berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

    Dikelompokkan berdasarkan: Label keparahan

    Menemukan filter:

    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

25. Ember S3 teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis sumber daya adalah `AwsS3Bucket`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

26. Instans EC2 teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Jenis sumber daya adalah `AwsEc2Instance`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

27. AMI teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

    Dikelompokkan berdasarkan: ID gambar instans EC2

    Menemukan filter:

    - Jenis sumber daya adalah `AwsEc2Instance`

- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

28. Pengguna IAM teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

    Dikelompokkan berdasarkan: ID kunci akses IAM

    Menemukan filter:

    - Jenis sumber daya adalah `AwsIamAccessKey`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

29. Sumber daya teratas berdasarkan jumlah pemeriksaan CIS yang gagal

    ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

    Dikelompokkan berdasarkan: Resource ID

    Menemukan filter:

    - Generator ID dimulai dengan `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
    - Diperbarui di hari terakhir
    - Status kepatuhan adalah `FAILED`
    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

30. Integrasi teratas berdasarkan jumlah temuan

    ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

    Dikelompokkan berdasarkan: Produk ARN

    Menemukan filter:

    - Record state adalah `ACTIVE`
    - Status alur kerja adalah `NEW` atau `NOTIFIED`

31. Sumber daya dengan pemeriksaan keamanan paling gagal

    ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- Diperbarui di hari terakhir
- Status kepatuhan adalah `FAILED`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

32. Pengguna IAM dengan aktivitas mencurigakan

ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

Dikelompokkan berdasarkan: Pengguna IAM

Menemukan filter:

- Jenis sumber daya adalah `AwsIamUser`
- Record state adalah `ACTIVE`
- Status alur kerja adalah `NEW` atau `NOTIFIED`

33. Sumber daya dengan AWS Health temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- `ProductName`sama `Health`

34. Sumber daya dengan AWS Config temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

Dikelompokkan berdasarkan: Resource ID

Menemukan filter:

- `ProductName`sama `Config`

35. Aplikasi dengan temuan terbanyak

ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

Dikelompokkan berdasarkan: ResourceApplicationArn

Menemukan filter:

- `RecordState`sama `ACTIVE`
- `Workflow.Status`sama `NEW` atau `NOTIFIED`

Memahami wawasan khusus di Security Hub CSPM

Selain wawasan terkelola AWS Security Hub CSPM, Anda dapat membuat wawasan khusus di Security Hub CSPM untuk melacak masalah yang spesifik untuk lingkungan Anda. Wawasan khusus membantu Anda melacak subset masalah yang dikuratori.

Berikut adalah beberapa contoh wawasan khusus yang mungkin berguna untuk disiapkan:

- Jika Anda memiliki akun administrator, Anda dapat mengatur wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi yang memengaruhi akun anggota.
- Jika Anda mengandalkan AWS layanan terintegrasi tertentu, Anda dapat menyiapkan wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi dari layanan tersebut.
- Jika Anda mengandalkan integrasi pihak ketiga, Anda dapat menyiapkan wawasan khusus untuk melacak temuan kritis dan tingkat keparahan tinggi dari produk terintegrasi tersebut.

Anda dapat membuat wawasan kustom yang benar-benar baru, atau mulai dari wawasan kustom atau terkelola yang ada.

Setiap wawasan dapat dikonfigurasi dengan opsi berikut:

- Atribut pengelompokan — Atribut pengelompokan menentukan item mana yang ditampilkan dalam daftar hasil wawasan. Misalnya, jika atribut pengelompokan adalah Nama Produk, hasil wawasan menampilkan jumlah temuan yang terkait dengan setiap penyedia temuan.
- Filter opsional — Filter mempersempit temuan yang cocok untuk wawasan.

  Temuan disertakan dalam hasil wawasan hanya jika cocok dengan semua filter yang disediakan. Misalnya, jika filter adalah “Nama produk adalah GuardDuty" dan “Jenis sumber daya adalah `AwsS3Bucket` “, temuan yang cocok harus sesuai dengan kedua kriteria ini.

  Namun, Security Hub CSPM menerapkan logika BOolean OR ke filter yang menggunakan atribut yang sama tetapi nilai yang berbeda. Misalnya, jika filter adalah “Nama produk adalah GuardDuty" dan “Nama produk adalah Amazon Inspector”, penemuan cocok jika dibuat oleh Amazon GuardDuty atau Amazon Inspector.

Jika Anda menggunakan pengidentifikasi sumber daya atau jenis sumber daya sebagai atribut pengelompokan, hasil wawasan mencakup semua sumber daya yang ada dalam temuan yang cocok. Daftar ini tidak terbatas pada sumber daya yang cocok dengan filter jenis sumber daya. Misalnya, wawasan mengidentifikasi temuan yang terkait dengan bucket S3, dan mengelompokkan temuan tersebut berdasarkan pengidentifikasi sumber daya. Temuan yang cocok berisi sumber daya bucket S3 dan sumber daya kunci akses IAM. Hasil wawasan mencakup kedua sumber daya.

Jika Anda mengaktifkan agregasi lintas wilayah dan kemudian membuat wawasan khusus, wawasan akan berlaku untuk pencocokan temuan di Wilayah agregasi dan Wilayah tertaut. Pengecualiannya adalah jika wawasan Anda menyertakan filter Wilayah.

Membuat wawasan khusus

Di AWS Security Hub CSPM, wawasan khusus dapat digunakan untuk mengumpulkan serangkaian temuan tertentu dan melacak masalah yang unik untuk lingkungan Anda. Untuk informasi latar belakang tentang wawasan khusus, lihatMemahami wawasan khusus di Security Hub CSPM.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk membuat wawasan khusus di Security Hub CSPM

Security Hub CSPM console

Untuk membuat wawasan khusus (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pilih Buat wawasan.
4. Untuk memilih atribut pengelompokan untuk wawasan:
    a. Pilih kotak pencarian untuk menampilkan opsi filter.
    b. Pilih Grup berdasarkan.
    c. Pilih atribut yang akan digunakan untuk mengelompokkan temuan yang terkait dengan wawasan ini.
    d. Pilih Terapkan.
5. Secara opsional, pilih filter tambahan apa pun yang akan digunakan untuk wawasan ini. Untuk setiap filter, tentukan kriteria filter, lalu pilih Ter apkan.
6. Pilih Buat wawasan.
7. Masukkan nama Insight, lalu pilih Buat wawasan.

Security Hub CSPM API

Untuk membuat wawasan khusus (API)

1. Untuk membuat wawasan khusus, gunakan pen CreateInsight goperasian Security Hub CSPM API. Jika Anda menggunakan AWS CLI, jalankan create-insight perintah.
2. Isi `Name` parameter dengan nama untuk wawasan kustom Anda.
3. Isi `Filters` parameter untuk menentukan temuan mana yang akan dimasukkan dalam wawasan.
4. Isi `GroupByAttribute` parameter untuk menentukan atribut mana yang digunakan untuk mengelompokkan temuan yang disertakan dalam wawasan.
5. Secara opsional, isi `SortCriteria` parameter untuk mengurutkan temuan berdasarkan bidang tertentu.

Contoh berikut membuat wawasan khusus yang mencakup temuan penting dengan jenis `AwsIamRole` sumber daya. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

Untuk membuat wawasan khusus (PowerShell)

1. Gunakan `New-SHUBInsight` cmdlet.
2. Isi `Name` parameter dengan nama untuk wawasan kustom Anda.
3. Isi `Filter` parameter untuk menentukan temuan mana yang akan dimasukkan dalam wawasan.
4. Isi `GroupByAttribute` parameter untuk menentukan atribut mana yang digunakan untuk mengelompokkan temuan yang disertakan dalam wawasan.

Jika Anda telah mengaktifkan agregasi lintas wilayah dan menggunakan cmdlet ini dari Wilayah agregasi, wawasan akan berlaku untuk pencocokan temuan dari agregasi dan Wilayah tertaut.

Contoh

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Membuat wawasan khusus dari wawasan terkelola (hanya konsol)

Anda tidak dapat menyimpan perubahan atau menghapus wawasan terkelola. Namun, Anda dapat menggunakan wawasan terkelola sebagai dasar untuk wawasan khusus. Ini adalah opsi pada konsol CSPM Security Hub saja.

Untuk membuat wawasan khusus dari wawasan terkelola (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pilih wawasan terkelola untuk bekerja.
4. Edit konfigurasi wawasan sesuai kebutuhan.
   - Untuk mengubah atribut yang digunakan untuk mengelompokkan temuan dalam wawasan:
     a. Untuk menghapus pengelompokan yang ada, pilih X di sebelah Grup dengan pengaturan.
     b. Pilih kotak pencarian.
     c. Pilih atribut yang akan digunakan untuk pengelompokan.
     d. Pilih Terapkan.
   - Untuk menghapus filter dari wawasan, pilih X yang dilingkari di sebelah filter.
   - Untuk menambahkan filter ke wawasan:
     a. Pilih kotak pencarian.
     b. Pilih atribut dan nilai yang akan digunakan sebagai filter.

c. Pilih Terapkan.

5. Setelah pembaruan selesai, pilih Buat wawasan.
6. Saat diminta, masukkan nama Insight, lalu pilih Buat wawasan.

Mengedit wawasan khusus

Anda dapat mengedit wawasan kustom yang ada untuk mengubah nilai pengelompokan dan filter. Setelah Anda membuat perubahan, Anda dapat menyimpan pembaruan ke wawasan asli, atau menyimpan versi yang diperbarui sebagai wawasan baru.

Di AWS Security Hub CSPM, wawasan khusus dapat digunakan untuk mengumpulkan serangkaian temuan tertentu dan melacak masalah yang unik untuk lingkungan Anda. Untuk informasi latar belakang tentang wawasan khusus, lihatMemahami wawasan khusus di Security Hub CSPM.

Untuk mengedit wawasan khusus, pilih metode pilihan Anda, dan ikuti petunjuknya.

Security Hub CSPM console

Untuk mengedit wawasan khusus (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pilih wawasan khusus untuk dimodifikasi.
4. Edit konfigurasi wawasan sesuai kebutuhan.
   - Untuk mengubah atribut yang digunakan untuk mengelompokkan temuan dalam wawasan:
     a. Untuk menghapus pengelompokan yang ada, pilih X di sebelah Grup dengan pengaturan.
     b. Pilih kotak pencarian.
     c. Pilih atribut yang akan digunakan untuk pengelompokan.
     d. Pilih Terapkan.
   - Untuk menghapus filter dari wawasan, pilih X yang dilingkari di sebelah filter.
   - Untuk menambahkan filter ke wawasan:
     a. Pilih kotak pencarian.
     b. Pilih atribut dan nilai yang akan digunakan sebagai filter.
     c. Pilih Terapkan.

5. Saat Anda menyelesaikan pembaruan, pilih S impan wawasan.
6. Saat diminta, lakukan salah satu hal berikut:
   - Untuk memperbarui wawasan yang ada agar mencerminkan perubahan Anda, pilih Per barui, ***<Insight_Name>*** lalu pilih S impan wawasan.
   - Untuk membuat wawasan baru dengan pembaruan, pilih S impan wawasan baru. Masukkan nama Insight, lalu pilih S impan wawasan.

Security Hub CSPM API

Untuk mengedit wawasan khusus (API)

1. Gunakan pen `UpdateInsight` goperasian Security Hub CSPM API. Jika Anda menggunakan update-insight perintah AWS CLI jalankan.
2. Untuk mengidentifikasi wawasan khusus yang ingin Anda perbarui, berikan Nama Sumber Daya Amazon (ARN) wawasan tersebut. Untuk mendapatkan ARN wawasan khusus, gunakan `GetInsights` operasi atau get-insights perintah.
3. Perbarui `GroupByAttribute` parameter `NameFilters`,, dan sesuai kebutuhan.

Contoh berikut memperbarui wawasan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" --filters '{"ResourceType": [{ "Comparison": "EQUALS", "Value":
 "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --
name "High severity role findings"
```

PowerShell

Untuk mengedit wawasan khusus (PowerShell)

1. Gunakan `Update-SHUBInsight` cmdlet.
2. Untuk mengidentifikasi wawasan khusus, berikan Nama Sumber Daya Amazon (ARN) wawasan tersebut. Untuk mendapatkan ARN wawasan khusus, gunakan `Get-SHUBInsight` cmdlet.
3. Perbarui `GroupByAttribute` parameter `NameFilter`,, dan sesuai kebutuhan.

Contoh

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Menghapus wawasan khusus

Di AWS Security Hub CSPM, wawasan khusus dapat digunakan untuk mengumpulkan serangkaian temuan tertentu dan melacak masalah yang unik untuk lingkungan Anda. Untuk informasi latar belakang tentang wawasan khusus, lihatMemahami wawasan khusus di Security Hub CSPM.

Untuk menghapus wawasan khusus, pilih metode pilihan Anda, dan ikuti petunjuknya. Anda tidak dapat menghapus wawasan terkelola.

Security Hub CSPM console

Untuk menghapus wawasan khusus (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, silakan pilih Wawasan.
3. Temukan wawasan khusus untuk dihapus.
4. Untuk wawasan itu, pilih ikon opsi lainnya (tiga titik di sudut kanan atas kartu).
5. Pilih Hapus.

Security Hub CSPM API

Untuk menghapus wawasan kustom (API)

1. Gunakan pen `DeleteInsight` goperasian Security Hub CSPM API. Jika Anda menggunakan delete-insight perintah AWS CLI jalankan.
2. Untuk mengidentifikasi wawasan khusus yang akan dihapus, berikan ARN wawasan. Untuk mendapatkan ARN wawasan khusus, gunakan `GetInsights` operasi atau get-insights perintah.

Contoh berikut menghapus wawasan yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

Untuk menghapus wawasan khusus (PowerShell)

1. Gunakan `Remove-SHUBInsight` cmdlet.
2. Untuk mengidentifikasi wawasan khusus, berikan ARN wawasan. Untuk mendapatkan ARN wawasan khusus, gunakan `Get-SHUBInsight` cmdlet.

Contoh

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Secara otomatis memodifikasi dan bertindak atas temuan di Security Hub CSPM

AWSSecurity Hub CSPM memiliki fitur yang secara otomatis memodifikasi dan mengambil tindakan atas temuan berdasarkan spesifikasi Anda.

Security Hub CSPM saat ini mendukung dua jenis otomatisasi:

- Aturan otomatisasi — Memperbarui dan menekan temuan secara otomatis dalam waktu dekat berdasarkan kriteria yang Anda tentukan.
- Respons dan remediasi otomatis — Buat EventBridge aturan Amazon khusus yang menentukan tindakan otomatis yang harus diambil terhadap temuan dan wawasan tertentu.

Aturan otomatisasi sangat membantu saat Anda ingin memperbarui bidang pencarian secara otomatis di AWS Security Finding Format (ASFF). Misalnya, Anda dapat menggunakan aturan otomatisasi untuk memperbarui tingkat keparahan atau status alur kerja temuan dari integrasi pihak ketiga tertentu. Menggunakan aturan otomatisasi menghilangkan kebutuhan untuk memperbarui tingkat keparahan atau status alur kerja secara manual dari setiap temuan dari produk pihak ketiga ini.

EventBridge aturan sangat membantu ketika Anda ingin mengambil tindakan di luar CSPM Security Hub sehubungan dengan temuan spesifik atau mengirimkan temuan spesifik ke alat pihak ketiga untuk remediasi atau penyelidikan tambahan. Aturan dapat digunakan untuk memicu tindakan yang didukung, seperti menjalankan AWS Lambda fungsi atau memberi tahu topik Amazon Simple Notification Service (Amazon SNS) tentang temuan tertentu.

Aturan otomatisasi berlaku sebelum EventBridge aturan diterapkan. Artinya, aturan otomatisasi dipicu dan memperbarui temuan sebelum EventBridge menerima temuan. EventBridge aturan kemudian berlaku untuk temuan yang diperbarui.

Saat menyiapkan otomatisasi untuk kontrol keamanan, sebaiknya filter berdasarkan ID kontrol daripada judul atau deskripsi. Sedangkan Security Hub CSPM terkadang memperbarui judul dan deskripsi kontrol, ID kontrol tetap sama.

Topik

- Memahami aturan otomatisasi di Security Hub CSPM
- Menggunakan EventBridge untuk respon otomatis dan remediasi

Memahami aturan otomatisasi di Security Hub CSPM

Anda dapat menggunakan aturan otomatisasi untuk memperbarui temuan secara otomatis di AWS Security Hub CSPM. Saat mencerna temuan, Security Hub CSPM dapat menerapkan berbagai tindakan aturan, seperti menekan temuan, mengubah tingkat keparahannya, dan menambahkan catatan. Tindakan aturan tersebut mengubah temuan yang sesuai dengan kriteria yang Anda tentukan.

Contoh kasus penggunaan untuk aturan otomatisasi meliputi:

- Meningkatkan keparahan temuan `CRITICAL` jika ID sumber daya temuan mengacu pada sumber daya bisnis yang penting.
- Meningkatkan keparahan temuan dari `HIGH` `CRITICAL` jika temuan tersebut memengaruhi sumber daya dalam akun produksi tertentu.
- Menetapkan temuan spesifik yang memiliki tingkat keparahan status `INFORMATIONAL` `SUPPRESSED` alur kerja.

Anda dapat membuat dan mengelola aturan otomatisasi hanya dari akun administrator CSPM Security Hub.

Aturan berlaku untuk temuan baru dan temuan terbaru. Anda dapat membuat aturan kustom dari awal, atau menggunakan templat aturan yang disediakan oleh Security Hub CSPM. Anda juga dapat memulai dengan template dan memodifikasinya sesuai kebutuhan.

Mendefinisikan kriteria aturan dan tindakan aturan

Dari akun administrator CSPM Security Hub, Anda dapat membuat aturan otomatisasi dengan menentukan satu atau beberapa kriteria aturan dan satu atau beberapa tindakan aturan. Ketika temuan cocok dengan kriteria yang ditentukan, Security Hub CSPM menerapkan tindakan aturan untuk itu. Untuk informasi selengkapnya tentang kriteria dan tindakan yang tersedia, lihatKriteria aturan dan tindakan aturan yang tersedia.

Security Hub CSPM saat ini mendukung maksimal 100 aturan otomatisasi untuk setiap akun administrator.

Akun administrator CSPM Security Hub juga dapat mengedit, melihat, dan menghapus aturan otomatisasi. Aturan berlaku untuk pencocokan temuan di akun administrator dan semua akun anggotanya. Dengan memberikan ID akun anggota sebagai kriteria aturan, administrator CSPM Security Hub juga dapat menggunakan aturan otomatisasi untuk memperbarui atau menekan temuan di akun anggota tertentu.

Aturan otomatisasi hanya berlaku Wilayah AWS di tempat pembuatannya. Untuk menerapkan aturan di beberapa Wilayah, administrator harus membuat aturan di setiap Wilayah. Ini dapat dilakukan melalui konsol CSPM Security Hub, Security Hub CSPM API, atau. AWS CloudFormation Anda juga dapat menggunakan skrip penyebaran Multi-wilayah.

Kriteria aturan dan tindakan aturan yang tersedia

Bidang AWS Security Finding Format (ASFF) berikut saat ini didukung sebagai kriteria untuk aturan otomatisasi:

Kriteria aturan	Operator filter	Jenis bidang
`AwsAccountId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`AwsAccountName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`CompanyName`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`ComplianceAssociatedStandardsId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`ComplianceSecurityControlId`	`CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS`	String
`ComplianceStatus`	`Is, Is Not`	Pilih: [`FAILED`,`NOT_AVAILABLE` ,`PASSED`,`WARNING`]
`Confidence`	`Eq (equal-to), Gte (greater-than-equa`	Bilangan

Kriteria aturan	Operator filter	Jenis bidang
	l), Lte (less-than-equal)	
CreatedAt	Start, End, DateRange	Tanggal (diformat sebagai T21:47:39.269Z 2022-12-01)
Criticality	Eq (equal-to), Gte (greater-than-equa l), Lte (less-than-equal)	Bilangan
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String
FirstObservedAt	Start, End, DateRange	Tanggal (diformat sebagai T21:47:39.269Z 2022-12-01)
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String
LastObservedAt	Start, End, DateRange	Tanggal (diformat sebagai T21:47:39.269Z 2022-12-01)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String

Kriteria aturan	Operator filter	Jenis bidang
NoteUpdatedAt	Start, End, DateRange	Tanggal (diformat sebagai T21:47:39.269Z 2022-12-01)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String

Kriteria aturan	Operator filter	Jenis bidang
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	String
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
ResourceType	Is, Is Not	Pilih (lihat Sumber yang didukung oleh ASFF)

Kriteria aturan	Operator filter	Jenis bidang
SeverityLabel	Is, Is Not	Pilih: [CRITICAL,HIGH,MEDIUM,LOW,INFORM ONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String
UpdatedAt	Start, End, DateRange	Tanggal (diformat sebagai T21:47:39.269Z 2022-12-01)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Peta
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NO T_EQUALS	String
WorkflowStatus	Is, Is Not	Pilih: [NEW,NOTIFIED,RESOLVED,SUPPRESS D]

Untuk kriteria yang diberi label sebagai bidang string, menggunakan operator filter yang berbeda pada bidang yang sama memengaruhi logika evaluasi. Untuk informasi selengkapnya, lihat StringFilterdi Referensi API CSPM AWS Security Hub.

Setiap kriteria mendukung jumlah maksimum nilai yang dapat digunakan untuk menyaring temuan yang cocok. Untuk batasan pada setiap kriteria, lihat AutomationRulesFindingFiltersdi Referensi API CSPM AWS Security Hub.

Bidang ASFF berikut saat ini didukung sebagai tindakan untuk aturan otomatisasi:

- `Confidence`
- `Criticality`
- `Note`
- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Untuk informasi selengkapnya tentang bidang ASFF tertentu, lihat sintaks AWSSecurity Finding Format (ASFF).

> **Tip**
>
> Jika Anda ingin Security Hub CSPM berhenti menghasilkan temuan untuk kontrol tertentu, sebaiknya nonaktifkan kontrol daripada menggunakan aturan otomatisasi. Ketika Anda menonaktifkan kontrol, Security Hub CSPM berhenti menjalankan pemeriksaan keamanan di atasnya dan berhenti menghasilkan temuan untuk itu, sehingga Anda tidak akan dikenakan biaya untuk kontrol itu. Sebaiknya gunakan aturan otomatisasi untuk mengubah nilai bidang ASFF tertentu untuk temuan yang sesuai dengan kriteria yang ditentukan. Untuk informasi selengkapnya tentang menonaktifkan kontrol, lihat. Menonaktifkan kontrol di Security Hub CSPM

Temuan yang dievaluasi oleh aturan otomatisasi

Aturan otomatisasi mengevaluasi temuan baru dan terbaru yang dihasilkan atau dicerna oleh Security Hub CSPM melalui BatchImportFindingsoperasi setelah Anda membuat aturan. Security Hub CSPM memperbarui temuan kontrol setiap 12-24 jam atau ketika sumber daya terkait berubah status. Untuk informasi selengkapnya, lihat Jadwal untuk menjalankan pemeriksaan keamanan.

Aturan otomatisasi mengevaluasi temuan asli yang disediakan penyedia. Penyedia dapat menyediakan temuan baru dan memperbarui temuan yang ada dengan menggunakan `BatchImportFindings` pengoperasian Security Hub CSPM API. Jika bidang berikut tidak ada dalam temuan asli, Security Hub CSPM secara otomatis mengisi bidang dan kemudian menggunakan nilai yang terisi dalam evaluasi dengan aturan otomatisasi:

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`
- `Workflow.Status`

Setelah Anda membuat satu atau beberapa aturan otomatisasi, aturan tidak akan dipicu jika Anda memperbarui bidang pencarian menggunakan BatchUpdateFindingsoperasi. Jika Anda membuat aturan otomatisasi dan membuat `BatchUpdateFindings` pembaruan yang memengaruhi bidang temuan yang sama, pembaruan terakhir akan menetapkan nilai untuk bidang tersebut. Ambil contoh berikut:

1. Anda menggunakan `BatchUpdateFindings` operasi untuk mengubah nilai `Workflow.Status` bidang temuan dari `NEW` ke`NOTIFIED`.
2. Jika Anda meneleponGetFindings, `Workflow.Status` bidang sekarang memiliki nilai`NOTIFIED`.
3. Anda membuat aturan otomatisasi yang mengubah `Workflow.Status` bidang temuan dari `NEW` ke`SUPPRESSED`. (Ingat bahwa aturan mengabaikan pembaruan yang dibuat menggunakan `BatchUpdateFindings` operasi.)
4. Penyedia temuan menggunakan `BatchImportFindings` operasi untuk memperbarui temuan dan mengubah nilai untuk `Workflow.Status` bidang temuan ke`NEW`.

5. Jika Anda meneleponGetFindings, Workflow.Status bidang sekarang memiliki nilaiSUPPRESSED. Ini adalah kasus karena aturan otomatisasi diterapkan, dan aturan adalah tindakan terakhir yang diambil pada temuan tersebut.

Saat Anda membuat atau mengedit aturan di konsol CSPM Security Hub, konsol akan menampilkan beta temuan yang sesuai dengan kriteria aturan. Sementara aturan otomatisasi mengevaluasi temuan asli yang dikirim oleh penyedia temuan, beta konsol mencerminkan temuan dalam keadaan akhir mereka karena akan ditampilkan dalam respons terhadap GetFindingsoperasi (yaitu, setelah tindakan aturan atau pembaruan lain diterapkan pada temuan).

Cara kerja urutan aturan

Saat membuat aturan otomatisasi, Anda menetapkan setiap aturan pesanan. Ini menentukan urutan di mana Security Hub CSPM menerapkan aturan otomatisasi Anda, dan menjadi penting ketika beberapa aturan terkait dengan bidang temuan atau pencarian yang sama.

Ketika beberapa tindakan aturan berhubungan dengan bidang temuan atau pencarian yang sama, aturan dengan nilai numerik tertinggi untuk urutan aturan berlaku terakhir dan memiliki efek akhir.

Saat Anda membuat aturan di konsol CSPM Security Hub, Security Hub CSPM secara otomatis menetapkan urutan aturan berdasarkan urutan pembuatan aturan. Aturan yang paling baru dibuat memiliki nilai numerik terendah untuk urutan aturan dan oleh karena itu berlaku terlebih dahulu. Security Hub CSPM menerapkan aturan berikutnya dalam urutan menaik.

Bila Anda membuat aturan melalui Security Hub CSPM API atauAWS CLI, Security Hub CSPM menerapkan aturan dengan nilai numerik terendah untuk pertama. RuleOrder Ini kemudian menerapkan aturan selanjutnya dalam urutan menaik. Jika beberapa temuan memiliki hal yang samaRuleOrder, Security Hub CSPM menerapkan aturan dengan nilai sebelumnya untuk UpdatedAt bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

Anda dapat mengubah urutan aturan kapan saja.

Contoh urutan aturan:

Aturan A (urutan aturan adalah**1**):

- Kriteria Aturan A
  - ProductName = Security Hub CSPM
  - Resources.Typeadalah S3 Bucket

  - `Compliance.Status` = `FAILED`
  - `RecordState`adalah `NEW`
  - `Workflow.Status` = `ACTIVE`
- Aturan A tindakan
  - Perbarui `Confidence` ke `95`
  - Perbarui `Severity` ke `CRITICAL`

Aturan B (urutan aturan adalah**2**):

- Kriteria aturan B
  - `AwsAccountId` = `123456789012`
- Tindakan aturan B
  - Perbarui `Severity` ke `INFORMATIONAL`

Aturan Tindakan diterapkan terlebih dahulu pada temuan CSPM Security Hub yang cocok dengan kriteria Aturan A. Selanjutnya, tindakan Aturan B berlaku untuk temuan CSPM Security Hub dengan ID akun yang ditentukan. Dalam contoh ini, karena Aturan B berlaku terakhir, nilai akhir `Severity` dalam temuan dari ID akun yang ditentukan adalah`INFORMATIONAL`. Berdasarkan tindakan Aturan A, nilai akhir dari temuan `Confidence` yang cocok adalah`95`.

Membuat aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub CSPM. Anda dapat membuat aturan otomatisasi kustom dari awal atau, di konsol CSPM Security Hub, gunakan templat aturan yang telah diisi sebelumnya. Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihat[Memahami aturan otomatisasi di Security Hub CSPM](#).

Anda hanya dapat membuat satu aturan otomatisasi pada satu waktu. Untuk membuat beberapa aturan otomatisasi, ikuti prosedur konsol beberapa kali, atau panggil API atau perintah beberapa kali dengan parameter yang Anda inginkan.

Anda harus membuat aturan otomatisasi di setiap Wilayah dan akun di mana Anda ingin aturan tersebut diterapkan pada temuan.

Saat Anda membuat aturan otomatisasi di konsol CSPM Security Hub, Security Hub CSPM menunjukkan versi beta dari temuan yang diterapkan aturan Anda. Beta saat ini tidak didukung jika

kriteria aturan Anda menyertakan filter CONTAINS atau NOT_CONTAINS. Anda dapat memilih filter ini untuk jenis bidang peta dan string.

> **Important**
>
> AWSmerekomendasikan agar Anda tidak menyertakan informasi identitas pribadi, rahasia, atau sensitif dalam nama aturan, deskripsi, atau bidang lainnya.

Membuat aturan otomatisasi khusus

Pilih metode pilihan Anda, dan selesaikan langkah-langkah berikut untuk membuat aturan otomatisasi kustom.

Console

Untuk membuat aturan otomatisasi kustom (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol CSPM Security Hub AWS di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Otomasi.
3. Pilih Buat aturan. Untuk Jenis Aturan, pilih Buat aturan kustom.
4. Di bagian Aturan, berikan nama aturan unik dan deskripsi untuk aturan Anda.
5. Untuk Kriteria, gunakan menu tarik-turun Kunci, Operator, dan Nilai untuk menentukan kriteria aturan Anda. Anda harus menentukan setidaknya satu kriteria aturan.

   Jika didukung untuk kriteria yang Anda pilih, konsol akan menampilkan beta temuan yang sesuai dengan kriteria Anda.
6. Untuk tindakan Otomatis, gunakan menu tarik-turun untuk menentukan bidang pencarian mana yang akan diperbarui saat temuan cocok dengan kriteria aturan Anda. Anda harus menentukan setidaknya satu tindakan aturan.
7. Untuk status Aturan, pilih apakah Anda ingin aturan Diaktifkan atau Dinonaktifkan setelah dibuat.
8. (Opsional) Perluas bagian Pengaturan tambahan. Pilih Abaikan aturan berikutnya untuk temuan yang cocok dengan kriteria ini jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.

9. (Opsional) Untuk Tag, tambahkan tag sebagai pasangan nilai kunci untuk membantu Anda mengidentifikasi aturan dengan mudah.
10. Pilih Buat aturan.

API

Untuk membuat aturan otomatisasi kustom (API)

1. Jalankan `CreateAutomationRule`dari akun administrator CSPM Security Hub. API ini membuat aturan dengan Amazon Resource Name (ARN) tertentu.
2. Sediakan nama dan deskripsi untuk aturan.
3. Tetapkan `IsTerminal` parameter ke `true` jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
4. Untuk `RuleOrder` parameter, berikan urutan aturan. Security Hub CSPM menerapkan aturan dengan nilai numerik yang lebih rendah untuk parameter ini terlebih dahulu.
5. Untuk `RuleStatus` parameter, tentukan apakah Anda ingin CSPM Security Hub mengaktifkan dan mulai menerapkan aturan ke temuan setelah pembuatan. Jika tidak ada nilai yang ditentukan, nilai defaultnya adalah `ENABLED`. Nilai `DISABLED` berarti bahwa aturan dijeda setelah penciptaan.
6. Untuk `Criteria` parameternya, berikan kriteria yang ingin digunakan CSPM Security Hub untuk memfilter temuan Anda. Tindakan aturan akan berlaku untuk temuan yang sesuai dengan kriteria. Untuk daftar kriteria yang didukung, lihatKriteria aturan dan tindakan aturan yang tersedia.
7. Untuk `Actions` parameternya, berikan tindakan yang ingin dilakukan CSPM Security Hub saat ada kecocokan antara temuan dan kriteria yang ditentukan. Untuk daftar tindakan yang didukung, lihatKriteria aturan dan tindakan aturan yang tersedia.

Contoh AWS CLI perintah berikut membuat aturan otomatisasi memperbarui status alur kerja dan catatan temuan yang cocok. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-automation-rule \
--actions '[{
 "Type": "FINDING_FIELDS_UPDATE",
 "FindingFieldsUpdate": {
 "Severity": {
```

```
 "Label": "HIGH"
 },
 "Note": {
 "Text": "Known issue that is a risk. Updated by automation rules",
 "UpdatedBy": "sechub-automation"
 }
 }
 }]' \
--criteria '{
 "SeverityLabel": [{
 "Value": "INFORMATIONAL",
 "Comparison": "EQUALS"
 }]
 }' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Membuat aturan otomatisasi dari template (hanya konsol)

Template aturan mencerminkan kasus penggunaan umum untuk aturan otomatisasi. Saat ini, hanya konsol CSPM Security Hub yang mendukung template aturan. Selesaikan langkah-langkah berikut untuk membuat aturan otomatisasi dari templat di konsol.

Untuk membuat aturan otomatisasi dari template (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol CSPM Security Hub AWS di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Otomasi.
3. Pilih Buat aturan. Untuk Jenis Aturan, pilih Buat aturan dari templat.
4. Pilih template aturan dari menu drop-down.
5. (Opsional) Jika perlu untuk kasus penggunaan Anda, ubah bagian Aturan, Kriteria, dan Tindakan Otomatis. Anda harus menentukan setidaknya satu kriteria aturan dan satu tindakan aturan.

   Jika didukung untuk kriteria yang Anda pilih, konsol akan menampilkan beta temuan yang sesuai dengan kriteria Anda.

6. Untuk status Aturan, pilih apakah Anda ingin aturan Diaktifkan atau Dinonaktifkan setelah dibuat.
7. (Opsional) Perluas bagian Pengaturan tambahan. Pilih Abaikan aturan berikutnya untuk temuan yang cocok dengan kriteria ini jika Anda ingin aturan ini menjadi aturan terakhir yang diterapkan pada temuan yang cocok dengan kriteria aturan.
8. (Opsional) Untuk Tag, tambahkan tag sebagai pasangan nilai kunci untuk membantu Anda mengidentifikasi aturan dengan mudah.
9. Pilih Buat aturan.

Melihat aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub CSPM. Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihatMemahami aturan otomatisasi di Security Hub CSPM.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk melihat aturan otomatisasi yang ada dan detail setiap aturan.

Untuk melihat riwayat bagaimana aturan otomatisasi telah mengubah temuan Anda, lihatMeninjau detail dan riwayat temuan di Security Hub CSPM.

Console

Untuk melihat aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol CSPM Security Hub AWS di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Otomasi.
3. Pilih nama aturan. Atau, pilih aturan.
4. Pilih Tindakan dan Tampilan.

API

Untuk melihat aturan otomatisasi (API)

1. Untuk melihat aturan otomatisasi akun Anda, jalankan `ListAutomationRules`dari akun administrator CSPM Security Hub. API ini mengembalikan aturan ARN dan metadata lainnya untuk aturan Anda. Tidak ada parameter input yang diperlukan untuk API ini, tetapi Anda

dapat secara opsional menyediakan `MaxResults` untuk membatasi jumlah hasil dan `NextToken` sebagai parameter pagination. Nilai awal `NextToken` harus`NULL`.

2. Untuk detail aturan tambahan, termasuk kriteria dan tindakan untuk aturan, jalankan `BatchGetAutomationRules`dari akun administrator CSPM Security Hub. Berikan ARN aturan otomatisasi yang Anda inginkan detailnya.

   Contoh berikut mengambil rincian untuk aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

   ```
   $ aws securityhub batch-get-automation-rules \
   --automation-rules-arns '["arn:aws:securityhub:us-
   east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
   cdef-EXAMPLE22222"]' \
   --region us-east-1
   ```

Mengedit aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub CSPM. Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihatMemahami aturan otomatisasi di Security Hub CSPM.

Setelah membuat aturan otomatisasi, administrator CSPM Security Hub yang didelegasikan dapat mengedit aturan. Saat Anda mengedit aturan otomatisasi, perubahan tersebut berlaku untuk temuan baru dan terbaru yang dihasilkan atau dicerna CSPM Security Hub setelah aturan diedit.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengedit konten aturan otomatisasi. Anda dapat mengedit satu atau beberapa aturan dengan satu permintaan. Untuk petunjuk tentang urutan aturan pengeditan, lihatMengedit urutan aturan otomatisasi.

Console

Untuk mengedit aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol CSPM Security Hub AWS di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Otomasi.
3. Pilih aturan yang ingin Anda edit. Pilih Tindakan dan Edit.

4. Ubah aturan sesuai keinginan, dan pilih Simpan perubahan.

API

Untuk mengedit aturan otomatisasi (API)

1. Jalankan `BatchUpdateAutomationRules`dari akun administrator CSPM Security Hub.
2. Untuk `RuleArn` parameter, berikan ARN dari aturan yang ingin Anda edit.
3. Berikan nilai baru untuk parameter yang ingin Anda edit. Anda dapat mengedit parameter apa pun kecuali`RuleArn`.

Contoh berikut memperbarui aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
    {
      "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
          "Note": {
            "Text": "Known issue that is a risk",
            "UpdatedBy": "sechub-automation"
          },
          "Workflow": {
            "Status": "NEW"
          }
        }
      }],
      "Criteria": {
        "SeverityLabel": [{
         "Value": "LOW",
         "Comparison": "EQUALS"
        }]
      },
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 14,
      "RuleStatus": "DISABLED",
```

```
    }
  ]' \
--region us-east-1
```

Mengedit urutan aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub CSPM. Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihatMemahami aturan otomatisasi di Security Hub CSPM.

Setelah membuat aturan otomatisasi, administrator CSPM Security Hub yang didelegasikan dapat mengedit aturan.

Jika Anda ingin menjaga kriteria aturan dan tindakan tetap sama, tetapi mengubah urutan di mana Security Hub CSPM menerapkan aturan otomatisasi, Anda dapat mengedit hanya urutan aturan. Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk mengedit urutan aturan.

Untuk petunjuk tentang mengedit kriteria atau tindakan aturan otomatisasi, lihatMengedit aturan otomatisasi.

Console

Untuk mengedit urutan aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol CSPM Security Hub AWS di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Otomasi.
3. Pilih aturan yang urutannya ingin Anda ubah. Pilih Edit prioritas.
4. Pilih Pindah ke atas untuk meningkatkan prioritas aturan dengan satu unit. Pilih Pindah ke bawah untuk mengurangi prioritas aturan sebanyak satu unit. Pilih Pindah ke atas untuk menetapkan aturan urutan 1 (ini memberikan aturan lebih diutamakan daripada aturan lain yang ada).

> **Note**
>
> Saat Anda membuat aturan di konsol CSPM Security Hub, Security Hub CSPM secara otomatis menetapkan urutan aturan berdasarkan urutan pembuatan aturan. Aturan yang

paling baru dibuat memiliki nilai numerik terendah untuk urutan aturan dan oleh karena itu berlaku terlebih dahulu.

API

Untuk mengedit urutan aturan otomatisasi (API)

1. Gunakan `BatchUpdateAutomationRules` operasi dari akun administrator CSPM Security Hub.
2. Untuk `RuleArn` parameternya, berikan ARN dari aturan yang urutannya ingin Anda edit.
3. Ubah nilai `RuleOrder` bidang.

> **Note**
>
> Jika beberapa aturan memiliki hal yang sama`RuleOrder`, Security Hub CSPM menerapkan aturan dengan nilai sebelumnya untuk `UpdatedAt` bidang terlebih dahulu (yaitu, aturan yang terakhir diedit berlaku terakhir).

Menghapus atau menonaktifkan aturan otomatisasi

Aturan otomatisasi dapat digunakan untuk memperbarui temuan secara otomatis di AWS Security Hub CSPM. Untuk informasi latar belakang tentang cara kerja aturan otomatisasi, lihatMemahami aturan otomatisasi di Security Hub CSPM.

Saat Anda menghapus aturan otomatisasi, Security Hub CSPM menghapusnya dari akun Anda dan tidak lagi menerapkan aturan tersebut pada temuan. Sebagai alternatif untuk penghapusan, Anda dapat menonaktifkan aturan. Ini mempertahankan aturan untuk penggunaan di masa mendatang, tetapi CSPM Security Hub tidak akan menerapkan aturan tersebut pada temuan yang cocok sampai Anda mengaktifkannya.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk menghapus aturan otomatisasi. Anda dapat menghapus satu atau beberapa aturan dalam satu permintaan.

Console

Untuk menghapus atau menonaktifkan aturan otomatisasi (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol CSPM Security Hub AWS di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Otomasi.
3. Pilih aturan yang ingin Anda hapus. Pilih Tindakan dan Hapus (untuk mempertahankan aturan, tetapi nonaktifkan sementara, pilih Nonaktifkan).
4. Konfirmasikan pilihan Anda, dan pilih Hapus.

API

Untuk menghapus atau menonaktifkan aturan otomatisasi (API)

1. Gunakan `BatchDeleteAutomationRules`operasi dari akun administrator CSPM Security Hub.
2. Untuk `AutomationRulesArns` parameter, berikan ARN dari aturan yang ingin Anda hapus (untuk mempertahankan aturan, tetapi nonaktifkan sementara, sediakan `DISABLED` `RuleStatus` parameternya).

Contoh berikut menghapus aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1
```

Contoh aturan otomatisasi

Bagian ini memberikan contoh aturan otomatisasi untuk kasus penggunaan CSPM Security Hub umum. Contoh-contoh ini sesuai dengan template aturan yang tersedia di konsol CSPM Security Hub.

Tingkatkan tingkat keparahan menjadi Kritis saat sumber daya tertentu seperti bucket S3 berisiko

Dalam contoh ini, kriteria aturan dicocokkan ketika `ResourceId` dalam temuan adalah bucket Amazon Simple Storage Service (Amazon S3) tertentu. Tindakan aturannya adalah mengubah tingkat keparahan temuan yang cocok menjadi`CRITICAL`. Anda dapat memodifikasi template ini untuk diterapkan ke sumber daya lain.

Contoh permintaan API:

```
{
    "IsTerminal": true,
    "RuleName": "Elevate severity of findings that relate to important resources",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity to CRITICAL when specific resource such as
 an S3 bucket is at risk",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "ResourceId": [{
            "Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
```

```
            },
            "Note": {
                "Text": "This is a critical resource. Please review ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Contoh perintah CLI:

```
$
aws securityhub create-automation-rule \
--is-terminal \
--rule-name "Elevate severity of findings that relate to important resources" \
--rule-order 1 \
--rule-status "ENABLED" \

--description "Elevate finding severity to CRITICAL when specific resource such as an
 S3 bucket is at risk" \
--criteria '{
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"ResourceId": [{
"Value": "arn:aws:s3:::amzn-s3-demo-bucket/developers/design_info.doc",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
```

```
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "This is a critical resource. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Meningkatkan keparahan temuan yang berhubungan dengan sumber daya dalam akun produksi

Dalam contoh ini, kriteria aturan dicocokkan ketika temuan `HIGH` tingkat keparahan dihasilkan di akun produksi tertentu. Tindakan aturannya adalah mengubah tingkat keparahan temuan yang cocok menjadi`CRITICAL`.

Contoh permintaan API:

```
{
    "IsTerminal": false,
    "RuleName": "Elevate severity for production accounts",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Elevate finding severity from HIGH to CRITICAL for findings that
 relate to resources in specific production accounts",
    "Criteria": {
        "ProductName": [{
            "Value": "Security Hub CSPM",
            "Comparison": "EQUALS"
        }],
        "ComplianceStatus": [{
            "Value": "FAILED",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
```

```
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "HIGH",
            "Comparison": "EQUALS"
        }],
        "AwsAccountId": [
        {
            "Value": "111122223333",
            "Comparison": "EQUALS"
        },
        {
            "Value": "123456789012",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Severity": {
                "Label": "CRITICAL"
            },
            "Note": {
                "Text": "A resource in production accounts is at risk. Please review
 ASAP.",
                "UpdatedBy": "sechub-automation"
            }
        }
    }]
}
```

Contoh perintah CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
 accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
 to resources in specific production accounts" \
--criteria '{
```

```
"ProductName": [{
"Value": "Security Hub CSPM",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Menekan temuan informasi

Dalam contoh ini, kriteria aturan dicocokkan untuk temuan `INFORMATIONAL` tingkat keparahan yang dikirim ke Security Hub CSPM dari Amazon. GuardDuty Tindakan aturannya adalah mengubah status alur kerja dari temuan yang cocok menjadi. `SUPPRESSED`

Contoh permintaan API:

```
{
    "IsTerminal": false,
    "RuleName": "Suppress informational findings",
    "RuleOrder": 1,
    "RuleStatus": "ENABLED",
    "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
    "Criteria": {
        "ProductName": [{
            "Value": "GuardDuty",
            "Comparison": "EQUALS"
        }],
        "RecordState": [{
            "Value": "ACTIVE",
            "Comparison": "EQUALS"
        }],
        "WorkflowStatus": [{
            "Value": "NEW",
            "Comparison": "EQUALS"
        }],
        "SeverityLabel": [{
            "Value": "INFORMATIONAL",
            "Comparison": "EQUALS"
        }]
    },
    "Actions": [{
        "Type": "FINDING_FIELDS_UPDATE",
        "FindingFieldsUpdate": {
            "Workflow": {
                "Status": "SUPPRESSED"
            },
            "Note": {
                "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
 severity",
                "UpdatedBy": "sechub-automation"
            }
```

```
        }
    }]
}
```

Contoh perintah CLI:

```
aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"WorkflowStatus": [{
"Value": "NEW",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{
"Value": "INFORMATIONAL",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Workflow": {
"Status": "SUPPRESSED"
},
"Note": {
"Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
```

```
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1
```

Menggunakan EventBridge untuk respon otomatis dan remediasi

Dengan membuat aturan di Amazon EventBridge, Anda dapat merespons temuan CSPM AWS Security Hub secara otomatis. Security Hub CSPM mengirimkan temuan sebagai peristiwa ke EventBridge dalam waktu hampir real time. Anda dapat menulis aturan sederhana untuk menunjukkan peristiwa mana yang Anda minati dan tindakan otomatis apa yang harus diambil ketika suatu peristiwa cocok dengan aturan. Tindakan yang dapat dipicu secara otomatis meliputi hal-hal berikut:

- Memanggil fungsi AWS Lambda
- Memanggil perintah run Amazon EC2
- Mengirim peristiwa ke Amazon Kinesis Data Streams
- Mengaktifkan mesin AWS Step Functions status
- Memberi tahu topik Amazon SNS atau antrean Amazon SQS
- Mengirim temuan ke alat manajemen tiket, obrolan, SIEM, atau respon insiden pihak ketiga

Security Hub CSPM secara otomatis mengirimkan semua temuan baru dan semua pembaruan untuk temuan yang ada ke acara EventBridge as EventBridge . Anda juga dapat membuat tindakan khusus yang memungkinkan Anda mengirim temuan dan hasil wawasan yang dipilih ke EventBridge.

Anda kemudian mengkonfigurasi EventBridge aturan untuk merespons setiap jenis peristiwa.

Untuk informasi selengkapnya tentang penggunaan EventBridge, lihat Panduan EventBridge Pengguna Amazon .

> **Note**
>
> Sebagai praktik terbaik, pastikan bahwa izin yang diberikan kepada pengguna Anda untuk mengakses EventBridge menggunakan kebijakan hak istimewa terkecil AWS Identity and Access Management (IAM) yang hanya memberikan izin yang diperlukan.
> Untuk informasi selengkapnya, lihat Identitas dan manajemen akses di Amazon EventBridge.

Satu set templat untuk respons dan remediasi otomatis lintas akun juga tersedia di AWS Solusi. Template memanfaatkan aturan EventBridge acara dan fungsi Lambda. Anda menyebarkan solusi menggunakan CloudFormation dan AWS Systems Manager. Solusinya dapat menciptakan respons dan tindakan remediasi yang sepenuhnya otomatis. Ini juga dapat menggunakan tindakan kustom Security Hub CSPM untuk membuat respons dan tindakan remediasi yang dipicu pengguna. Untuk detail tentang cara mengonfigurasi dan menggunakan solusi, lihat Respon Keamanan Otomatis pada halaman AWS solusi.

Topik

- Jenis acara CSPM Hub Keamanan di EventBridge
- EventBridge format acara untuk Security Hub CSPM
- Mengkonfigurasi EventBridge aturan untuk temuan CSPM Security Hub
- Menggunakan tindakan khusus untuk mengirim hasil temuan dan wawasan ke EventBridge

Jenis acara CSPM Hub Keamanan di EventBridge

Security Hub CSPM menggunakan jenis EventBridge acara Amazon berikut untuk diintegrasikan. EventBridge

Pada EventBridge dasbor untuk Security Hub CSPM, Semua Acara menyer takan semua jenis acara ini.

Semua temuan (Temuan Hub Keamanan - Diimpor)

Security Hub CSPM secara otomatis mengirimkan semua temuan baru dan semua pembaruan untuk temuan yang ada ke acara EventBridge as Security Hub Findings - Imported. Setiap Security Hub Findings - Imported peristiwa berisi satu temuan.

Setiap `BatchImportFindings` `BatchUpdateFindings` permintaan memicu Security Hub Findings - Imported peristiwa.

Untuk akun administrator, umpan acara menyer EventBridge takan peristiwa untuk temuan dari akun mereka dan dari akun anggota mereka.

Di Wilayah agregasi, umpan peristiwa menyertakan peristiwa untuk temuan dari Wilayah agregasi dan Wilayah yang ditautkan. Cross-Region temuan disertakan dalam umpan acara hampir secara real time. Untuk informasi tentang cara mengonfigurasi agregasi pencarian, lihatthe section called “Menggabungkan data di seluruh Wilayah”.

Anda dapat menentukan aturan EventBridge yang secara otomatis merutekan temuan ke alur kerja remediasi, alat pihak ketiga, atau EventBridge target https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-targets.html lain yang didukung. Aturan dapat menyertakan filter yang hanya menerapkan aturan jika temuan memiliki nilai atribut tertentu.

Anda menggunakan metode ini untuk secara otomatis mengirim semua temuan, atau semua temuan yang memiliki karakteristik tertentu, ke alur kerja respons atau remediasi.

Lihat the section called “Mengkonfigurasi EventBridge aturan”.

Temuan untuk tindakan khusus (Temuan Hub Keamanan - Tindakan Kustom)

Security Hub CSPM juga mengirimkan temuan yang terkait dengan tindakan kustom ke acara EventBridge as Security Hub Findings - Custom Action.

Ini berguna bagi analis yang bekerja dengan konsol CSPM Security Hub yang ingin mengirim temuan tertentu, atau serangkaian kecil temuan, ke alur kerja respons atau remediasi. Anda dapat memilih tindakan kustom hingga 20 temuan sekaligus. Setiap temuan dikirim EventBridge sebagai EventBridge acara terpisah.

Saat Anda membuat tindakan kustom, Anda menetapkannya sebagai ID tindakan kustom. Anda dapat menggunakan ID ini untuk membuat EventBridge aturan yang mengambil tindakan tertentu setelah menerima temuan yang terkait dengan ID tindakan kustom tersebut.

Lihat the section called “Mengkonfigurasi dan menggunakan tindakan khusus”.

Misalnya, Anda dapat membuat tindakan kustom di Security Hub CSPM yang disebut. `send_to_ticketing` Kemudian EventBridge, Anda membuat aturan yang dipicu saat EventBridge menerima temuan yang menyertakan ID tindakan `send_to_ticketing` kustom. Aturannya mencakup logika untuk mengirim temuan ke sistem tiket Anda. Anda kemudian dapat memilih temuan dalam Security Hub CSPM dan menggunakan tindakan kustom di Security Hub CSPM untuk mengirim temuan secara manual ke sistem tiket Anda.

Untuk contoh cara mengirim temuan CSPM Hub Keamanan EventBridge untuk diproses lebih lanjut, lihat Cara Mengintegrasikan Tindakan Kustom CSPM Hub AWS Keamanan dengan PagerDuty dan Cara Mengaktifkan Tindakan Kustom di AWS Security Hub CSPM di Blog Jaringan AWS Mitra (APN).

Hasil wawasan untuk tindakan khusus (Hasil Wawasan Hub Keamanan)

Anda juga dapat menggunakan tindakan khusus untuk mengirim kumpulan hasil wawasan ke Security Hub Insight Results acara EventBridge sebagai. Hasil wawasan adalah sumber daya yang

cocok dengan wawasan. Perhatikan bahwa ketika Anda mengirim hasil wawasan ke EventBridge, Anda tidak mengirimkan temuan ke EventBridge. Anda hanya mengirim pengidentifikasi sumber daya yang terkait dengan hasil wawasan. Anda dapat mengirim hingga 100 pengidentifikasi sumber daya sekaligus.

Mirip dengan tindakan kustom untuk temuan, pertama-tama Anda membuat tindakan kustom di Security Hub CSPM, lalu membuat aturan di. EventBridge

Lihat the section called “Mengkonfigurasi dan menggunakan tindakan khusus”.

Misalnya, Anda melihat hasil wawasan tertentu yang menarik yang ingin Anda bagikan dengan rekan kerja. Dalam hal ini, Anda dapat menggunakan tindakan khusus untuk mengirimkan hasil wawasan tersebut kepada kolega melalui sistem obrolan atau tiket.

EventBridge format acara untuk Security Hub CSPM

Jenis Security Hub Findings - Imported Security Findings - Custom Action,, dan Security Hub Insight Results acara menggunakan format acara berikut.

Format acara adalah format yang digunakan saat Security Hub CSPM mengirim acara ke. EventBridge

Temuan Hub Keamanan - Diimpor

Security Hub Findings - Importedperistiwa yang dikirim dari Security Hub CSPM untuk EventBridge menggunakan format berikut.

```
{
   "version":"0",
   "id":"CWE-event-id",
   "detail-type":"Security Hub Findings - Imported",
   "source":"aws.securityhub",
   "account":"111122223333",
   "time":"2019-04-11T21:52:17Z",
   "region":"us-west-2",
   "resources":[
      "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-
west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/
f2893b211841"
   ],
   "detail":{
      "findings": [{
         <finding content>
```

```
        }]
    }
}
```

*<finding content>*adalah konten, dalam format JSON, dari temuan yang dikirim oleh acara tersebut. Setiap peristiwa mengirimkan satu temuan.

Untuk daftar lengkap atribut pencarian, lihatAWS Format Penemuan Keamanan (ASFF).

Untuk informasi tentang cara mengonfigurasi EventBridge aturan yang dipicu oleh peristiwa ini, lihatthe section called “Mengkonfigurasi EventBridge aturan”.

Temuan Hub Keamanan - Tindakan Kustom

Security Hub Findings - Custom Actionperistiwa yang dikirim dari Security Hub CSPM untuk EventBridge menggunakan format berikut. Setiap temuan dikirim dalam acara terpisah.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName":"custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

*<finding content>*adalah konten, dalam format JSON, dari temuan yang dikirim oleh acara tersebut. Setiap peristiwa mengirimkan satu temuan.

Untuk daftar lengkap atribut pencarian, lihatAWS Format Penemuan Keamanan (ASFF).

Untuk informasi tentang cara mengonfigurasi EventBridge aturan yang dipicu oleh peristiwa ini, lihatthe section called “Mengkonfigurasi dan menggunakan tindakan khusus”.

Hasil Wawasan Hub Keamanan

Security Hub Insight Resultsperistiwa yang dikirim dari Security Hub CSPM untuk EventBridge menggunakan format berikut.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Insight Results",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2017-12-22T18:43:48Z",
  "region": "us-west-1",
  "resources": [
      "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
  ],
  "detail": {
    "actionName":"name of the action",
    "actionDescription":"description of the action",
    "insightArn":"ARN of the insight",
    "insightName":"Name of the insight",
    "resultType":"ResourceAwsIamAccessKeyUserName",
    "number of results":"number of results, max of 100",
    "insightResults": [
        {"result 1": 5},
        {"result 2": 6}
    ]
  }
}
```

Untuk informasi tentang cara membuat EventBridge aturan yang dipicu oleh peristiwa ini, lihatthe section called “Mengkonfigurasi dan menggunakan tindakan khusus”.

Mengkonfigurasi EventBridge aturan untuk temuan CSPM Security Hub

Anda dapat membuat aturan di Amazon EventBridge yang menentukan tindakan yang harus diambil saat Security Hub Findings - Imported acara diterima. Security Hub Findings - Importedperistiwa dipicu oleh pembaruan dari `BatchUpdateFindings` operasi `BatchImportFindings` dan.

Setiap aturan berisi pola peristiwa, yang mengidentifikasi peristiwa yang memicu aturan. Pola acara selalu berisi sumber peristiwa (`aws.securityhub`) dan jenis peristiwa (Temuan Hub Keamanan - Diimpor). Pola peristiwa juga dapat menentukan filter untuk mengidentifikasi temuan yang berlaku aturan.

Aturan acara kemudian mengidentifikasi target aturan. Target adalah tindakan yang harus diambil saat EventBridge menerima peristiwa Temuan Hub Keamanan - Imp or dan temuan tersebut cocok dengan filter.

Instruksi yang diberikan di sini menggunakan EventBridge konsol. Saat Anda menggunakan konsol, EventBridge secara otomatis membuat kebijakan berbasis sumber daya yang diperlukan yang memungkinkan EventBridge untuk menulis ke Amazon CloudWatch Log.

Anda juga dapat menggunakan `PutRule` operasi EventBridge API. Namun, jika Anda menggunakan EventBridge API, maka Anda harus membuat kebijakan berbasis sumber daya. Untuk informasi tentang kebijakan yang diperlukan, lihat CloudWatch Iz in log di Panduan EventBridge Pengguna Amazon.

Format pola acara

Format pola acara untuk Temuan Hub Keamanan - Event yang diimpor adalah sebagai berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`mengidentifikasi Security Hub CSPM sebagai layanan yang menghasilkan peristiwa.
- `detail-type`mengidentifikasi jenis peristiwa.
- `detail`bersifat opsional dan menyediakan nilai filter untuk pola acara. Jika pola peristiwa tidak berisi `detail` bidang, maka semua temuan memicu aturan.

Anda dapat memfilter temuan berdasarkan atribut pencarian apa pun. Untuk setiap atribut, Anda menyediakan array yang dipisahkan koma dari satu atau lebih nilai.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

Jika Anda memberikan lebih dari satu nilai untuk atribut, maka nilai-nilai tersebut digabungkan dengan`OR`. Penemuan cocok dengan filter untuk atribut individual jika temuan memiliki salah satu nilai yang tercantum. Misalnya, jika Anda memberikan keduanya `INFORMATIONAL` dan `LOW` sebagai nilai untuk`Severity.Label`, maka temuan cocok jika memiliki label keparahan salah satu `INFORMATIONAL` atau`LOW`.

Atribut bergabung dengan`AND`. Penemuan cocok jika cocok dengan kriteria filter untuk semua atribut yang disediakan.

Saat Anda memberikan nilai atribut, nilai tersebut harus mencerminkan lokasi atribut tersebut dalam struktur AWS Security Finding Format (ASFF).

> **Tip**
>
> Saat memfilter temuan kontrol, sebaiknya gunakan bidang `SecurityControlId` atau `SecurityControlArn` ASFF sebagai filter, bukan `Title` atau`Description`. Bidang terakhir dapat berubah sesekali, sedangkan ID kontrol dan ARN adalah pengidentifikasi statis.

Dalam contoh berikut, pola peristiwa memberikan nilai filter untuk `ProductArn` dan`Severity.Label`, jadi temuan cocok jika dibuat oleh Amazon Inspector dan memiliki label keparahan salah satu `INFORMATIONAL` atau`LOW`.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Security Hub Findings - Imported"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
```

```
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

Membuat aturan acara

Anda dapat menggunakan pola peristiwa yang telah ditentukan atau pola peristiwa khusus untuk membuat aturan di EventBridge. Jika Anda memilih pola yang telah ditentukan, EventBridge secara otomatis mengisi `source` dan`detail-type`. EventBridge juga menyediakan bidang untuk menentukan nilai filter untuk atribut pencarian berikut:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Untuk membuat EventBridge aturan (konsol)

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Menggunakan nilai-nilai berikut, buat EventBridge aturan yang memantau peristiwa pencarian:
   - Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
   - Pilih cara membangun pola acara.

Untuk membangun pola acara dengan...	Lakukan ini...	
Sebuah templat	Di bagian Pola acara, pilih opsi berikut: • Untuk Sumber peristiwa, pilih Layanan AWS . • Untuk AWS layanan, pilih Hub Keamanan. • Untuk Jenis Acara, pilih Temuan Hub Keamanan - Diimpor. • (Opsional) Untuk membuat aturan lebih spesifik, tambahkan nilai filter. Misalnya, untuk membatasi aturan pada temuan dengan status rekaman aktif, untuk status Rekaman Khusus, pilih Aktif.	

Untuk membangun pola acara dengan...	Lakukan ini...	
Pola acara khusus (Gunakan pola khusus jika Anda ingin memfilter temuan berdasarkan atribut yang tidak muncul di EventBridge konsol.)	• Di bagian Pola acara, pilih Pola khusus (editor JSON), lalu tempel pola peristiwa berikut ke area teks: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>" ] } } }` • Perbarui pola peristiwa untuk menyertakan nilai atribut dan atribut yang ingin Anda gunakan sebagai filter. Misalnya, untuk menerapkan aturan pada temuan yang memiliki status verifikasi `TRUE_POSITIVE` ,	

Untuk membangun pola acara dengan...	Lakukan ini...	
	gunakan contoh pola berikut: `{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "VerificationState": ["TRUE_POSITIVE"] } } }`	

- Untuk Jenis Target, pilih AWS layanan, dan untuk Pilih target, pilih target seperti topik atau AWS Lambda fungsi Amazon SNS. Target terpicu saat peristiwa diterima yang sesuai dengan pola peristiwa yang ditentukan dalam aturan.

Untuk detail tentang membuat aturan, lihat Membuat EventBridge aturan Amazon yang bereaksi terhadap peristiwa di Panduan EventBridge Pengguna Amazon.

Menggunakan tindakan khusus untuk mengirim hasil temuan dan wawasan ke EventBridge

Untuk menggunakan tindakan kustom AWS Security Hub CSPM untuk mengirim hasil temuan atau wawasan ke Amazon EventBridge, pertama-tama Anda membuat tindakan kustom di Security Hub CSPM. Kemudian, Anda dapat menentukan aturan EventBridge yang berlaku untuk tindakan kustom Anda.

Anda dapat membuat hingga 50 tindakan kustom.

Jika Anda mengaktifkan agregasi lintas wilayah, dan mengelola temuan dari Wilayah agregasi, maka buat tindakan kustom di Wilayah agregasi.

Aturan dalam EventBridge menggunakan Nama Sumber Daya Amazon (ARN) dari tindakan kustom.

Membuat tindakan kustom

Saat Anda membuat tindakan kustom di AWS Security Hub CSPM, Anda menentukan nama, deskripsi, dan pengidentifikasi uniknya.

Tindakan kustom menentukan tindakan yang harus diambil ketika suatu EventBridge peristiwa cocok dengan EventBridge aturan. Security Hub CSPM mengirimkan setiap temuan EventBridge sebagai acara.

Pilih metode pilihan Anda, dan ikuti langkah-langkah untuk membuat tindakan khusus.

Console

Untuk membuat tindakan kustom di Security Hub CSPM (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Peng aturan dan kemudian pilih Tind akan khusus.
3. Pilih Buat tindakan kustom.
4. Berikan Nama, Deskripsi, dan ID tindakan K ustom untuk tindakan tersebut.

   Nama harus kurang dari 20 karakter.

   ID tindakan kustom harus unik untuk setiap AWS akun.
5. Pilih Buat tindakan kustom.
6. Catat tindakan K ustom ARN. Anda perlu menggunakan ARN saat membuat aturan untuk dikaitkan dengan tindakan ini di EventBridge.

API

Untuk membuat tindakan kustom (API)

Gunakan CreateActionTarget operasi. Jika Anda menggunakan AWS CLI, jalankan perintah create-ac tion-target.

Contoh berikut membuat tindakan kustom untuk mengirim temuan ke alat remediasi. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

Mendefinisikan aturan di EventBridge

Untuk memicu tindakan kustom di Amazon EventBridge, Anda harus membuat aturan yang sesuai di EventBridge. Definisi aturan menyertakan Nama Sumber Daya Amazon (ARN) dari tindakan kustom.

Pola acara untuk peristiwa Temuan Hub Keamanan - Tind akan Kustom memiliki format berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Pola acara untuk acara Security Hub Insight Results memiliki format berikut:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Dalam kedua pola, *<custom action ARN>* adalah ARN dari tindakan khusus. Anda dapat mengonfigurasi aturan yang berlaku untuk lebih dari satu tindakan kustom.

Instruksi yang diberikan di sini adalah untuk EventBridge konsol. Saat Anda menggunakan konsol, EventBridge secara otomatis membuat kebijakan berbasis sumber daya yang diperlukan yang memungkinkan EventBridge untuk menulis ke CloudWatch Log.

Anda juga dapat menggunakan operasi `PutRule` API dari EventBridge API. Namun, jika Anda menggunakan EventBridge API, maka Anda harus membuat kebijakan berbasis sumber daya. Untuk detail tentang kebijakan yang diperlukan, lihat CloudWatch Iz in log di Panduan EventBridge Pengguna Amazon.

Untuk menentukan aturan di EventBridge (EventBridge console)

1. Buka EventBridge konsol Amazon di https://console.aws.amazon.com/events/.
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi aturan.
5. Untuk bus acara, pilih bus acara yang ingin Anda kaitkan dengan aturan ini. Jika Anda ingin aturan ini mencocokkan peristiwa yang berasal dari akun Anda, pilih default. Saat layanan AWS di akun Anda menghasilkan kejadian, layanan tersebut akan selalu masuk ke bus kejadian default akun Anda.
6. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
7. Pilih Selanjutnya.
8. Untuk Sumber acara, pilih AWS acara.
9. Untuk P ola acara, pilih For mulir pola acara.
10. Untuk Sumber peristiwa, pilih Layanan AWS .
11. Untuk AWS layanan, pilih Hub Keamanan.
12. Untuk Jenis peristiwa, lakukan salah satu hal berikut:
    - Untuk membuat aturan yang akan diterapkan saat Anda mengirim temuan ke tindakan kustom, pilih Temuan Hub Keamanan - Tindakan Kustom.
    - Untuk membuat aturan yang akan diterapkan saat Anda mengirim hasil wawasan ke tindakan kustom, pilih Hasil Wawasan Hub Keamanan.
13. Pilih ARN tindakan kustom spesifik, tambahkan tindakan khusus ARN.

    Jika aturan berlaku untuk beberapa tindakan kustom, pilih Tambah untuk menambahkan lebih banyak ARN tindakan kustom.

14. Pilih Berikutnya.
15. Di bawah Pilih target, pilih dan konfigurasikan target yang akan dipanggil saat aturan ini dicocokkan.
16. Pilih Berikutnya.
17. (Opsional) Masukkan satu atau lebih tanda untuk aturan. Untuk informasi selengkapnya, lihat EventBridge tag Amazon di Panduan EventBridge Pengguna Amazon.
18. Pilih Berikutnya.
19. Tinjau detail aturan dan pilih Buat aturan.

    Saat Anda melakukan tindakan khusus pada hasil temuan atau wawasan di akun Anda, peristiwa dihasilkan di EventBridge.

Memilih tindakan khusus untuk hasil temuan dan wawasan

Setelah membuat tindakan kustom CSPM Hub AWS Keamanan dan EventBridge aturan Amazon, Anda dapat mengirim hasil temuan dan wawasan ke EventBridge untuk pengelolaan dan pemrosesan otomatis.

Acara dikirim EventBridge hanya di akun tempat mereka dilihat. Jika Anda melihat temuan menggunakan akun administrator, acara dikirim ke EventBridge akun administrator.

Agar panggilan AWS API efektif, implementasi kode target harus mengalihkan peran ke akun anggota. Ini juga berarti bahwa peran yang Anda alihkan harus dikerahkan ke setiap anggota di mana tindakan diperlukan.

Untuk mengirim temuan ke EventBridge (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Tampilkan daftar temuan:

   - Dari Temuan, Anda dapat melihat temuan dari semua integrasi dan kontrol produk yang diaktifkan.
   - Dari Standar keamanan, Anda dapat menavigasi ke daftar temuan yang dihasilkan dari kontrol tertentu. Untuk informasi selengkapnya, lihat Meninjau detail kontrol di Security Hub CSPM.
   - Dari Integrasi, Anda dapat menavigasi ke daftar temuan yang dihasilkan oleh integrasi yang diaktifkan. Untuk informasi selengkapnya, lihat Melihat temuan dari integrasi CSPM Security Hub.

- Dari Wawasan, Anda dapat menavigasi ke daftar temuan untuk hasil wawasan. Untuk informasi selengkapnya, lihat Meninjau dan bertindak berdasarkan wawasan di Security Hub CSPM.

3. Pilih temuan untuk dikirim EventBridge. Anda dapat memilih hingga 20 temuan sekaligus.
4. Dari Tind akan, pilih tindakan kustom yang selaras dengan EventBridge aturan yang akan diterapkan.

   Security Hub CSPM mengirimkan peristiwa Temuan Hub Keamanan - Tindakan Kustom terpisah untuk setiap temuan.

Untuk mengirim hasil wawasan ke EventBridge (konsol)

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Pada panel navigasi, silakan pilih Wawasan.
3. Pada halaman Wawasan, pilih wawasan yang menyertakan hasil yang akan dikirim EventBridge.
4. Pilih hasil wawasan untuk dikirim EventBridge. Anda dapat memilih hingga 20 hasil sekaligus.
5. Dari Tind akan, pilih tindakan kustom yang selaras dengan EventBridge aturan yang akan diterapkan.

Bekerja dengan dasbor di Security Hub CSPM

Pada konsol CSPM Security Hub, dasbor Ring kasan menampilkan ringkasan risiko, urutan serangan, dan cakupan keamanan Anda. Dasbor ini membantu Anda mengidentifikasi risiko dan urutan serangan berdasarkan tingkat keparahan dan cakupan akun untuk berbagai kemampuan keamanan. Setiap kali Anda membuka dasbor, itu akan disegarkan secara otomatis. Namun, perhatikan bahwa skor keamanan dan status kontrol diperbarui setiap 24 jam.

Anda dapat menyesuaikan dasbor Ring kasan dengan menambahkan dan menghapus widget keamanan yang berbeda darinya. Anda juga dapat menentukan kriteria filter untuk mengambil dan menampilkan jenis data tertentu. Jika Anda menyesuaikan dasbor, Security Hub menyimpan pengaturan penyesuaian Anda. Jika pengguna lain dari akun Anda menyesuaikan dasbor, perubahan mereka disimpan secara independen dari pengaturan penyesuaian Anda.

Jika Anda mengonfigurasi agregasi lintas wilayah di Security Hub CSPM, dasbor Ring kasan menampilkan data agregat Anda. Jika akun Anda adalah akun administrator yang didelegasikan

untuk organisasi, data tersebut mencakup temuan untuk akun Anda dan akun anggota Anda. Jika akun Anda adalah akun anggota atau akun mandiri, data tersebut mencakup temuan hanya untuk akun Anda.

Topik

- Widget yang tersedia untuk dasbor Ringkasan
- Memfilter dasbor Ringkasan di Security Hub CSPM
- Menyesuaikan dasbor Ringkasan di Security Hub CSPM

Widget yang tersedia untuk dasbor Ringkasan

Das bor Ring kasan mencakup widget yang mencerminkan lanskap ancaman keamanan cloud modern, dipandu oleh operasi keamanan dan pengalaman AWS pelanggan. Beberapa widget ditampilkan secara default sementara yang lain tidak. Anda dapat menyesuaikan tampilan dasbor Anda dengan menambahkan atau menghapus widget.

Untuk menambahkan widget, pilih Tambahkan widget di bagian atas dasbor. Anda kemudian dapat menelusuri daftar widget yang tersedia atau memasukkan judul widget di bilah pencarian. Saat Anda menemukan widget untuk ditambahkan, seret ke lokasi di mana Anda ingin muncul di dasbor. Untuk informasi selengkapnya, lihat Menyesuaikan dasbor.

Widget ditampilkan secara default

Secara default, dasbor Ring kasan menyertakan widget berikut.

Urutan ancaman teratas

Menampilkan urutan ancaman tingkat keparahan tertinggi. Temuan urutan ancaman, yang dikenal sebagai temuan urutan serangan di Amazon GuardDuty, menghubungkan beberapa peristiwa untuk mengidentifikasi potensi ancaman terhadap AWS lingkungan Anda. Urutan ancaman dapat mencakup perilaku serangan yang sedang berlangsung atau baru-baru ini (dalam jendela waktu 24 jam) di lingkungan Anda, yang pada gilirannya dapat menyebabkan kompromi lebih lanjut. Anda harus mengaktifkan GuardDuty dan GuardDuty S3 Protection untuk menerima temuan urutan ancaman di Security Hub CSPM.

Risiko teratas

Menampilkan ringkasan risiko teratas di lingkungan Anda. Bagian atas widget menunjukkan jumlah risiko pada setiap tingkat keparahan. Anda dapat memilih tingkat keparahan untuk

membuka halaman Risiko dengan risiko yang difilter ke tingkat keparahan yang dipilih. Risiko yang paling sering terjadi di lingkungan Anda muncul terlebih dahulu. Widget ini membantu Anda memprioritaskan risiko mana yang harus diitigasi.

Cakupan keamanan

Merangkum tingkat cakupan keamanan Anda, berdasarkan temuan kontrol cakupan. Kontrol cakupan memeriksa apakah suatu spesifik Layanan AWS dan kemampuannya diaktifkan (misalnya,[Macie.1] Amazon Macie harus diaktifkan). Widget ini membantu Anda memastikan bahwa Anda memiliki PASSED temuan untuk kontrol cakupan. Konsol Security Hub CSPM menyediakan tautan dari widget ini untuk membantu Anda mengaktifkan kemampuan keamanan yang hilang. Sebaiknya gunakan konfigurasi pusat untuk mengaktifkan kemampuan keamanan yang hilang di beberapa Akun AWS dan Wilayah AWS. Untuk informasi selengkapnya, lihat Memahami konfigurasi pusat di Security Hub CSPM.

Standar keamanan

Menampilkan skor keamanan ringkasan terbaru Anda dan skor keamanan untuk setiap standar CSPM Hub Keamanan. Skor keamanan, yang berkisar antara 0-100 persen, mewakili proporsi kontrol yang dilewati relatif terhadap semua kontrol yang Anda aktifkan. Untuk informasi lebih lanjut tentang skor ini, lihatMetode penghitungan skor keamanan. Widget ini membantu Anda memahami postur keamanan Anda secara keseluruhan.

Aset dengan temuan terbanyak

Memberikan gambaran umum tentang sumber daya, akun, dan aplikasi yang memiliki temuan terbanyak. Daftar diurutkan dalam urutan menurun berdasarkan jumlah temuan. Di widget, setiap tab menunjukkan enam item teratas dalam kategori itu, dikelompokkan berdasarkan tingkat keparahan dan jenis sumber daya. Jika Anda memilih angka di kolom Total temuan, Security Hub CSPM membuka halaman yang menampilkan temuan untuk aset tersebut. Widget ini membantu Anda dengan cepat mengidentifikasi aset inti mana yang memiliki potensi ancaman keamanan.

Temuan berdasarkan Wilayah

Menampilkan jumlah total temuan, dikelompokkan berdasarkan tingkat keparahan, di masing-masing Wilayah AWS di mana Security Hub CSPM diaktifkan. Widget ini membantu Anda mengidentifikasi masalah keamanan yang berpotensi mempengaruhi Wilayah tertentu. Jika Anda membuka dasbor di Wilayah agregasi Anda, widget ini membantu Anda memantau potensi masalah keamanan di setiap Wilayah yang ditautkan.

Jenis ancaman yang paling umum

Memberikan rincian 10 jenis ancaman paling umum di AWS lingkungan Anda. Ini termasuk ancaman seperti peningkatan hak istimewa, penggunaan kredenSIAL yang terbuka, atau komunikasi dengan alamat IP berbahaya.

Untuk melihat data ini, Amazon GuardDuty harus diaktifkan. Jika ya, pilih jenis ancaman di widget ini untuk membuka GuardDuty konsol dan meninjau temuan yang terkait dengan ancaman ini. Widget ini membantu Anda mengevaluasi potensi ancaman dalam konteks masalah keamanan lainnya.

Kerentanan perangkat lunak dengan eksploitasi

Memberikan ringkasan kerentanan perangkat lunak yang ada di AWS lingkungan Anda dan telah diketahui eksploitasi. Anda juga dapat meninjau rincian kerentanan yang memiliki dan tidak memiliki perbaikan yang tersedia.

Untuk melihat data ini, Amazon Inspector harus diaktifkan. Jika ya, pilih statistik di widget ini untuk membuka konsol Amazon Inspector dan tinjau detail lebih lanjut tentang kerentanan. Widget ini membantu Anda mengevaluasi kerentanan perangkat lunak dalam konteks masalah keamanan lainnya.

Temuan baru dari waktu ke waktu

Menunjukkan tren dalam jumlah temuan harian baru selama 90 hari terakhir. Anda dapat memecah data berdasarkan tingkat keparahan atau berdasarkan penyedia untuk konteks tambahan. Widget ini membantu Anda memahami jika menemukan volume melonjak atau turun pada waktu tertentu selama 90 hari terakhir.

Sumber daya dengan temuan terbanyak

Menyediakan ringkasan sumber daya yang menghasilkan temuan terbanyak, dipecah berdasarkan jenis sumber daya berikut: bucket Amazon Simple Storage Service (Amazon S3), instans Amazon Elastic Compute Cloud (Amazon EC2), dan AWS Lambda fungsi.

Di widget, setiap tab berfokus pada salah satu jenis sumber daya sebelumnya, mencantumkan 10 contoh sumber daya yang menghasilkan temuan terbanyak. Untuk meninjau temuan untuk sumber daya tertentu, pilih instance sumber daya. Widget ini membantu Anda melakukan triase temuan keamanan yang terkait dengan AWS sumber daya umum.

Widget tersembunyi secara default

Widget berikut juga tersedia untuk dasbor Ring kasan, tetapi disembunyikan secara default.

AMI dengan temuan terbanyak

Menyediakan daftar 10 Gambar Mesin Amazon (AMI) yang telah menghasilkan temuan terbanyak. Data ini hanya tersedia jika Amazon EC2 diaktifkan untuk akun Anda. Ini membantu Anda mengidentifikasi AMI mana yang menimbulkan risiko keamanan potensial.

Kepala sekolah IAM dengan temuan terbanyak

Menyediakan daftar 10 pengguna AWS Identity and Access Management (IAM) yang telah menghasilkan temuan terbanyak. Widget ini membantu Anda melakukan tugas administrasi dan penagihan. Ini menunjukkan kepada Anda pengguna mana yang paling berkontribusi pada penggunaan CSPM Security Hub.

Akun dengan temuan terbanyak (berdasarkan tingkat keparahan)

Menampilkan grafik dari 10 akun yang telah menghasilkan temuan terbanyak, dikelompokkan berdasarkan tingkat keparahan. Widget ini membantu Anda menentukan akun mana yang akan difokuskan pada upaya analisis dan remediasi.

Akun dengan temuan terbanyak (berdasarkan jenis sumber daya)

Menampilkan grafik dari 10 akun yang telah menghasilkan temuan terbanyak, dikelompokkan berdasarkan jenis sumber daya. Widget ini membantu Anda menentukan akun dan jenis sumber daya yang akan diprioritaskan untuk analisis dan remediasi.

Wawasan

Daftar lima wawasan yang dikelola CSPM Security Hub dan jumlah temuan yang dihasilkannya. Wawasan mengidentifikasi area keamanan tertentu yang membutuhkan perhatian.

Temuan terbaru dari AWS integrasi

Menampilkan jumlah temuan yang Anda terima di Security Hub CSPM dari terintegrasi. Layanan AWS Ini juga menunjukkan kapan Anda baru-baru ini menerima temuan dari setiap layanan terintegrasi. Widget ini menyediakan data temuan konsolidasi dari beberapa Layanan AWS. Untuk menelusuri, pilih layanan terintegrasi. Security Hub CSPM kemudian membuka konsol untuk layanan tersebut.

Memfilter dasbor Ringkasan di Security Hub CSPM

Anda dapat mengatur dasbor Ringkasan di konsol CSPM Security Hub sehingga hanya menyertakan data keamanan yang paling relevan bagi Anda. Misalnya, jika Anda anggota tim aplikasi, Anda dapat membuat tampilan khusus untuk aplikasi penting di lingkungan produksi Anda. Jika Anda anggota tim keamanan, Anda dapat membuat tampilan khusus yang membantu Anda fokus pada temuan tingkat keparahan tinggi.

Untuk membuat tampilan yang dikuratori ini, masukkan kriteria filter di kotak filter di atas dasbor. Jika Anda menerapkan kriteria filter, kriteria berlaku untuk semua data dan widget di dasbor, kecuali data di widget Standar W awasan dan Keamanan. Untuk daftar widget yang tersedia di dasbor, lihatWidget yang tersedia untuk dasbor Ringkasan.

Anda dapat memfilter data dengan menggunakan bidang berikut:

- Nama akun
- account-id
- Aplikasi ARN
- Nama aplikasi
- Nama produk (untuk produk pihak ketiga Layanan AWS atau yang mengirimkan temuan ke Security Hub CSPM)
- Status rekam
- Region
- Tanda sumber daya
- Kepelikan
- Status alur kerja

Secara default, data dasbor difilter menggunakan kriteria berikut: `Workflow.Status` is `NOTIFIED` or`NEW`, and `RecordState` is`ACTIVE`. Kriteria ini muncul di atas dasbor, di bawah kotak filter. Untuk menghapus kriteria ini, pilih X di token filter untuk kriteria yang ingin Anda hapus.

Jika Anda menerapkan kriteria filter yang ingin Anda gunakan lagi, Anda dapat menyimpannya sebagai kum pulan filter. Kumpulan filter adalah kumpulan kriteria filter yang Anda buat dan simpan untuk diterapkan kembali saat Anda meninjau data di dasbor Ring kasan. Anda dapat membuat dan menyimpan kumpulan filter yang menggunakan salah satu bidang yang tersedia kecuali bidang berikut: ARN aplikasi, nama aplikasi, dan tag sumber daya.

Membuat dan menyimpan set filter

Ikuti langkah-langkah ini untuk membuat dan menyimpan set filter.

Untuk membuat dan menyimpan kumpulan filter

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Ringkasan.
3. Di kotak filter di atas dasbor Ring kasan, masukkan kriteria filter untuk set filter.
4. Pada menu Hapus filter, pilih S impan set filter baru.
5. Dalam kotak dialog Simpan set filter, masukkan nama untuk set filter.
6. (Opsional) Untuk menggunakan filter yang ditetapkan secara default setiap kali Anda membuka halaman Ring kasan, pilih opsi untuk mengaturnya sebagai tampilan default.
7. Pilih Simpan.

Untuk beralih di antara set filter yang telah Anda buat dan simpan, gunakan menu Pilih set filter di atas dasbor Ringkasan. Saat Anda memilih kumpulan filter, Security Hub CSPM menerapkan kriteria dari set filter ke data di dasbor.

Memperbarui atau menghapus set filter

Ikuti langkah-langkah ini untuk memperbarui atau menghapus set filter yang ada. Jika Anda menghapus kumpulan filter yang saat ini disetel sebagai tampilan default dasbor Ringkasan, tampilan default Anda diatur ulang ke tampilan CSPM Hub Keamanan default.

Untuk memperbarui atau menghapus kumpulan filter

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Ringkasan.
3. Di menu Pilih set filter di atas halaman Ringkasan, pilih set filter.
4. Pada menu Hapus filter, lakukan salah satu hal berikut:
   - Untuk memperbarui kumpulan filter, pilih Per barui set filter saat ini. Kemudian, masukkan perubahan Anda di kotak dialog yang muncul.
   - Untuk menghapus set filter pilih H apus set filter saat ini. Kemudian, pilih Hapus di kotak dialog yang muncul.

Menyesuaikan dasbor Ringkasan di Security Hub CSPM

Anda dapat menyesuaikan dasbor Ringkasan di konsol CSPM Security Hub dengan beberapa cara. Misalnya, Anda dapat menambahkan dan menghapus widget dari dasbor. Anda juga dapat mengatur ulang dan mengubah ukuran widget di dasbor. Untuk daftar widget yang tersedia dan deskripsi masing-masing, lihatWidget yang tersedia untuk dasbor Ringkasan.

Jika Anda menyesuaikan dasbor, Security Hub CSPM segera menerapkan perubahan Anda dan menyimpan pengaturan dasbor baru Anda. Perubahan Anda berlaku untuk tampilan dasbor Anda di semua Wilayah AWS dan browser.

Untuk menyesuaikan Ringkasan dasbor

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pilih Ringkasan.
3. Lakukan salah satu langkah berikut ini:
   - Untuk menambahkan widget, pilih Tambahkan widget di sudut kanan atas halaman. Di bilah pencarian, masukkan judul widget untuk ditambahkan. Kemudian, seret widget ke lokasi yang Anda inginkan.
   - Untuk menghapus widget, pilih tiga titik di sudut kanan atas widget.
   - Untuk memindahkan widget, pilih pegangan di sudut kiri atas widget, lalu seret widget ke lokasi yang Anda inginkan.
   - Untuk mengubah ukuran widget, pilih pegangan pengubah ukuran di sudut kanan bawah widget. Seret tepi widget hingga widget adalah ukuran pilihan Anda.

Untuk kemudian mengembalikan pengaturan asli, pilih Reset ke tata letak default di bagian atas halaman.

Batas regional untuk Security Hub CSPM

Beberapa fitur CSPM AWS Security Hub hanya tersedia dalam kondisi tertentu. Wilayah AWS Bagian berikut menentukan batas Regional ini. Untuk daftar lengkap semua Wilayah tempat CSPM Security Hub saat ini tersedia, lihat titik akhir dan kuota AWS Security Hub di. Referensi Umum AWS

Cross-Region pembatasan agregasi

DiAWS GovCloud (US) Regions, agregasi lintas wilayah tersedia untuk temuan, menemukan pembaruan, dan wawasan hanya. AWS GovCloud (US) Regions Secara khusus, Anda dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan hanya antara Wilayah AWS GovCloud (US-East) dan AWS GovCloud (US-West).

Di Wilayah Tiongkok, agregasi lintas wilayah tersedia untuk temuan, menemukan pembaruan, dan wawasan di seluruh Wilayah Tiongkok saja. Secara khusus, Anda dapat mengumpulkan temuan, menemukan pembaruan, dan wawasan hanya antara Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia).

Anda tidak dapat menggunakan Wilayah yang dinonaktifkan secara default sebagai Wilayah agregasi Anda. Untuk daftar Wilayah yang dinonaktifkan secara default, lihat Mengaktifkan atau menonaktifkan Wilayah AWS di akun Anda di Panduan AWS Account Management Referensi.

Ketersediaan integrasi menurut Wilayah

Beberapa integrasi tidak tersedia di semuaWilayah AWS. Di konsol CSPM Security Hub, integrasi tidak akan muncul di halaman Integrasi jika tidak tersedia di Wilayah tempat Anda masuk saat ini.

Integrasi yang didukung di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia)

Di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia), Security Hub CSPM hanya mendukung integrasi berikut dengan: Layanan AWS

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer
- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems ManagerOpsCenter
- AWS Systems ManagerManajer Patch

Di Wilayah Tiongkok (Beijing) dan Tiongkok (Ningxia), Security Hub CSPM hanya mendukung integrasi pihak ketiga berikut:

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integrasi yang didukung diAWS GovCloud (US-East)andAWS GovCloud (US-West)Wilayah

Di AWS GovCloud (US-East) dan AWS GovCloud (US-West) Wilayah, Security Hub CSPM hanya mendukung integrasi berikut dengan: Layanan AWS

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- Penganalisis Akses IAM
- Amazon Inspector
- AWS IoT Device Defender

Di AWS GovCloud (US-East) dan AWS GovCloud (US-West) Wilayah, Security Hub CSPM hanya mendukung integrasi pihak ketiga berikut:

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud

- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(hanya tersedia di AWS GovCloud (US-West))
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Ketersediaan standar menurut Wilayah

Standar yang AWS Control Tower dikelola layanan hanya tersedia dalam dukungan Wilayah AWS ituAWS Control Tower. Untuk daftar Wilayah yang AWS Control Tower saat ini mendukung, lihat Cara Wilayah AWS Bekerja Dengan AWS Control Tower di Panduan AWS Control Tower Pengguna.

Standar Penandaan AWS Sumber Daya tidak tersedia di Wilayah Asia Pasifik (Taipei).

Standar keamanan lainnya tersedia di semua Wilayah di mana Security Hub CSPM saat ini tersedia.

Ketersediaan kontrol berdasarkan Wilayah

Beberapa kontrol CSPM Security Hub tidak tersedia di semua. Wilayah AWS Untuk daftar kontrol yang tidak tersedia di setiap Wilayah, lihatBatasan regional pada kontrol CSPM Security Hub.

Di konsol CSPM Security Hub, kontrol tidak akan muncul di daftar kontrol jika tidak tersedia di Wilayah tempat Anda masuk saat ini. Pengecualian adalah Wilayah agregasi. Jika Anda menyetel Wilayah agregasi dan masuk ke Wilayah tersebut, konsol akan menampilkan kontrol yang tersedia di Wilayah agregasi atau satu atau beberapa Wilayah tertaut.

Batasan regional pada kontrol CSPM Security Hub

Beberapa kontrol CSPM AWS Security Hub tidak tersedia di semua. Wilayah AWS Halaman ini menentukan kontrol mana yang tidak tersedia di Wilayah tertentu.

Pada konsol CSPM Security Hub, kontrol tidak muncul dalam daftar kontrol jika tidak tersedia di Wilayah tempat Anda saat ini masuk. Pengecualiannya adalah Wilayah agregasi. Jika Anda menetapkan Wilayah agregasi dan masuk ke Wilayah tersebut, konsol akan menampilkan kontrol yang tersedia di Wilayah agregasi atau satu atau beberapa Wilayah tertaut.

Wilayah AWS

- AS Timur (Virginia Utara)
- AS Timur (Ohio)
- AS Barat (California Utara)
- AS Barat (Oregon)
- Africa (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Malaysia)
- Asia Pacific (Melbourne)
- Asia Pasifik (Mumbai)

- Asia Pasifik (Selandia Baru)
- Asia Pasifik (Osaka)
- Asia Pasifik (Seoul)
- Asia Pasifik (Singapura)
- Asia Pasifik (Sydney)
- Asia Pasifik (Taipei)
- Asia Pasifik (Thailand)
- Asia Pasifik (Tokyo)
- Kanada (Pusat)
- Kanada Barat (Calgary)
- Tiongkok (Beijing)
- Tiongkok (Ningxia)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Eropa (London)
- Europe (Milan)
- Eropa (Paris)
- Eropa (Spanyol)
- Eropa (Stockholm)
- Europe (Zurich)
- Israel (Tel Aviv)
- Meksiko (Tengah)
- Timur Tengah (Bahrain)
- Timur Tengah (UAE)
- Amerika Selatan (Sao Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

AS Timur (Virginia Utara)

Kontrol berikut tidak didukung di Wilayah AS Timur (Virginia Utara).

- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok

AS Timur (Ohio)

Kontrol berikut tidak didukung di Wilayah AS Timur (Ohio).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal

- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat

- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

AS Barat (California Utara)

Kontrol berikut tidak didukung di Wilayah AS Barat (California Utara).

- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada

- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus

- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

AS Barat (Oregon)

Kontrol berikut tidak didukung di Wilayah AS Barat (Oregon).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir

- [ECR.4] Repositori publik ECR harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Africa (Cape Town)

Kontrol berikut tidak didukung di Wilayah Afrika (Cape Town).

- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit

- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan

- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [ECR.4] Repositori publik ECR harus diberi tag
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai

- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [RDS.1] Snapshot RDS harus bersifat pribadi
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik

- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Asia Pasifik (Hong Kong)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Hong Kong).

- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai

- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal

- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag

- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat

- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Hyderabad)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Hyderabad).

- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai

- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien

- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan

- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus

- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer

- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat

- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Jakarta)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Jakarta).

- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit

- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai

- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager

- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [ECR.4] Repositori publik ECR harus diberi tag
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [GuardDuty.2] GuardDuty filter harus ditandai
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai

- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis

- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer

- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Malaysia)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Malaysia).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai

- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.2]AWS Backuppoin pemulihan harus ditandai
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan

- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.1] DataSync tugas harus mengaktifkan logging
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging

- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai

- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi

- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [ECS.19] Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi yang dikelola
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis
- [EFS.8] Sistem file EFS harus dienkripsi saat diam
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan

- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai

- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.1]AWS Gluepekerjaan harus diberi tag
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus

- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag

- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit

- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.38] RDS untuk instans DB PostgreSQL harus dienkripsi saat transit
- [RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit
- [RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch
- [RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung

- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok

- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik

- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pacific (Melbourne)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Melbourne).

- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit

- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager

- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik

- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM

- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag

- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit

- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus bersifat pribadi
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik

- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Mumbai)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Mumbai).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan

- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan

- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Asia Pasifik (Selandia Baru)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Selandia Baru).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.1] API Gateway REST dan logging eksekusi WebSocket API harus diaktifkan
- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [APIGateway.3] Tahap API REST API Gateway harus memiliki AWS X-Ray pelacakan diaktifkan
- [APIGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [APIGateway.5] Data cache API REST API Gateway harus dienkripsi saat diam
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi
- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.4]AWS AppSyncGraphQL API harus diberi tag
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Athena.2] Katalog data Athena harus ditandai
- [Athena.3] Kelompok kerja Athena harus ditandai
- [Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.2]AWS Backuppoin pemulihan harus ditandai
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan

- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.1] DataSync tugas harus mengaktifkan logging
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging

- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai

- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.172] Pengaturan Akses Publik Blok VPC EC2 harus memblokir lalu lintas gateway internet
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.182] Blokir pengaturan akses publik harus diaktifkan untuk snapshot Amazon EBS
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi

- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [ECS.18] Definisi Tugas ECS harus menggunakan enkripsi dalam transit untuk volume EFS
- [ECS.19] Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi yang dikelola
- [ECS.20] Definisi Tugas ECS harus mengkonfigurasi pengguna non-root dalam definisi wadah Linux
- [ECS.21] Definisi Tugas ECS harus mengkonfigurasi pengguna non-administrator dalam definisi wadah Windows
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis
- [EFS.8] Sistem file EFS harus dienkripsi saat diam
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung

- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Penyeimbang Beban Aplikasi harus dikaitkan dengan AWS WAF ACL web
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi
- [ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan

- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.1]AWS Gluepekerjaan harus diberi tag
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus ditandai
- [GuardDuty.3] GuardDuty IPset harus ditandai

- [GuardDuty.4] GuardDuty detektor harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan

- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag

- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat

- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai

- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.38] RDS untuk instans DB PostgreSQL harus dienkripsi saat transit
- [RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit
- [RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch
- [RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik

- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.13] Snapshot klaster Redshift harus diberi tag
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3

- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys

- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSOrganisasi saja
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.1] Instans Amazon EC2 harus dikelola olehAWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.1]AWS Transfer Familyalur kerja harus diberi tag
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan

- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11]AWS WAFpencatatan ACL web harus diaktifkan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Osaka)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Osaka).

- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging

- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis

- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai

- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan

- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Seoul)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Seoul).

- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai

- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [ECR.4] Repositori publik ECR harus diberi tag
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag

- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Asia Pasifik (Singapura)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Singapura).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus

- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat

- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Asia Pasifik (Sydney)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Sydney).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag

- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Asia Pasifik (Taipei)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Taipei).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [ACM.3] Sertifikat ACM harus ditandai
- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.1] API Gateway REST dan logging eksekusi WebSocket API harus diaktifkan
- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [APIGateway.3] Tahap API REST API Gateway harus memiliki AWS X-Ray pelacakan diaktifkan
- [APIGateway.4] API Gateway harus dikaitkan dengan ACL Web WAF
- [APIGateway.5] Data cache API REST API Gateway harus dienkripsi saat diam
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi

- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi
- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.4]AWS AppSyncGraphQL API harus diberi tag
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Athena.2] Katalog data Athena harus ditandai
- [Athena.3] Kelompok kerja Athena harus ditandai
- [Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan
- [AutoScaling.1] Grup Auto Scaling yang terkait dengan penyeimbang beban harus menggunakan pemeriksaan kesehatan ELB
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2

- [AutoScaling.10] Grup EC2 Auto Scaling harus diberi tag
- [Autoscaling.5] Instans Amazon EC2 yang diluncurkan menggunakan konfigurasi peluncuran grup Auto Scaling seharusnya tidak memiliki alamat IP Publik
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.2]AWS Backuppoin pemulihan harus ditandai
- [Backup.3]AWS Backupbrankas harus diberi tag
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Backup.5]AWS Backuprencana cadangan harus ditandai
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.2] CloudFormation tumpukan harus ditandai
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging

- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CloudTrail.9] CloudTrail jejak harus ditandai
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai

- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.1] DataSync tugas harus mengaktifkan logging
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.1] Instans replikasi Layanan Migrasi Database tidak boleh bersifat publik
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone

- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.5] Tabel DynamoDB harus diberi tag
- [DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.10] Amazon EC2 harus dikonfigurasi untuk menggunakan titik akhir VPC yang dibuat untuk layanan Amazon EC2
- [EC2.19] Kelompok keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.33] Lampiran gateway transit EC2 harus ditandai
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.35] Antarmuka jaringan EC2 harus ditandai

- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.37] Alamat IP Elastis EC2 harus ditandai
- [EC2.38] Instans EC2 harus ditandai
- [EC2.39] Gerbang internet EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.41] ACL jaringan EC2 harus ditandai
- [EC2.42] Tabel rute EC2 harus ditandai
- [EC2.43] Grup keamanan EC2 harus ditandai
- [EC2.44] Subnet EC2 harus ditandai
- [EC2.45] Volume EC2 harus ditandai
- [EC2.46] Amazon VPC harus ditandai
- [EC2.47] Layanan titik akhir Amazon VPC harus diberi tag
- [EC2.48] Log aliran VPC Amazon harus ditandai
- [EC2.49] Koneksi peering VPC Amazon harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.52] Gerbang transit EC2 harus ditandai
- [EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)

- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.172] Pengaturan Akses Publik Blok VPC EC2 harus memblokir lalu lintas gateway internet
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.182] Blokir pengaturan akses publik harus diaktifkan untuk snapshot Amazon EBS
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [ECS.2] Layanan ECS seharusnya tidak memiliki alamat IP publik yang ditetapkan kepadanya secara otomatis
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer

- [ECS.13] Layanan ECS harus ditandai
- [ECS.14] Cluster ECS harus ditandai
- [ECS.15] Definisi tugas ECS harus ditandai
- [ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [ECS.18] Definisi Tugas ECS harus menggunakan enkripsi dalam transit untuk volume EFS
- [ECS.19] Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi yang dikelola
- [ECS.20] Definisi Tugas ECS harus mengkonfigurasi pengguna non-root dalam definisi wadah Linux
- [ECS.21] Definisi Tugas ECS harus mengkonfigurasi pengguna non-administrator dalam definisi wadah Windows
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.5] Titik akses EFS harus diberi tag
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis
- [EFS.8] Sistem file EFS harus dienkripsi saat diam
- [EKS.1] Titik akhir cluster EKS tidak boleh diakses publik
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.6] Cluster EKS harus diberi tag
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager

- [ELB.3] Pendengar Classic Load Balancer harus dikonfigurasi dengan penghentian HTTPS atau TLS
- [ELB.7] Classic Load Balancer harus mengaktifkan pengeringan koneksi
- [ELB.8] Classic Load Balancer dengan pendengar SSL harus menggunakan kebijakan keamanan yang telah ditentukan sebelumnya yang memiliki kekuatan AWS Config urasi
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.16] Penyeimbang Beban Aplikasi harus dikaitkan dengan AWS WAF ACL web
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi
- [ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan

- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.1] Domain Elasticsearch harus mengaktifkan enkripsi saat istirahat
- [ES.2] Domain Elasticsearch seharusnya tidak dapat diakses publik
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [ES.5] Domain Elasticsearch harus mengaktifkan logging audit
- [ES.6] Domain Elasticsearch harus memiliki setidaknya tiga node data
- [ES.7] Domain Elasticsearch harus dikonfigurasi dengan setidaknya tiga node master khusus
- [ES.8] Koneksi ke domain Elasticsearch harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.2] bus EventBridge acara harus ditandai
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ

- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.1]AWS Gluepekerjaan harus diberi tag
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus ditandai
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai

- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [Kinesis.2] Aliran Kinesis harus ditandai
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.3]AWS KMS keystidak boleh dihapus secara tidak sengaja
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.6] Fungsi lambda harus ditandai
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan

- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.7] Firewall Firewall Jaringan harus ditandai
- [NetworkFirewall.8] Kebijakan firewall Network Firewall harus ditandai

- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.16] Cluster Aurora DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.17] Instans RDS DB harus dikonfigurasi untuk menyalin tag ke snapshot
- [RDS.19] Langganan pemberitahuan peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa cluster kritis
- [RDS.20] Langganan notifikasi peristiwa RDS yang ada harus dikonfigurasi untuk peristiwa instance database penting
- [RDS.21] Langganan pemberitahuan peristiwa RDS harus dikonfigurasi untuk peristiwa grup parameter basis data penting
- [RDS.22] Langganan notifikasi peristiwa RDS harus dikonfigurasi untuk peristiwa grup keamanan basis data penting
- [RDS.23] Instans RDS tidak boleh menggunakan port default mesin database
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus

- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.28] Cluster DB RDS harus diberi tag
- [RDS.29] Snapshot cluster RDS DB harus diberi tag
- [RDS.30] Instans DB RDS harus diberi tag
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.32] Snapshot DB RDS harus diberi tag
- [RDS.33] Grup subnet RDS DB harus diberi tag
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.38] RDS untuk instans DB PostgreSQL harus dienkripsi saat transit
- [RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit
- [RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch
- [RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis

- [Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.12] Langganan pemberitahuan acara Redshift harus ditandai
- [Redshift.13] Snapshot klaster Redshift harus diberi tag
- [Redshift.14] Grup subnet cluster Redshift harus diberi tag
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa

- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys
- [S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SecretsManager.1] Rahasia Secrets Manager harus mengaktifkan rotasi otomatis
- [SecretsManager.2] Rahasia Secrets Manager yang dikonfigurasi dengan rotasi otomatis harus berhasil diputar
- [SecretsManager.3] Hapus rahasia Secrets Manager yang tidak digunakan
- [SecretsManager.4] Rahasia Secrets Manager harus diputar dalam jumlah hari tertentu
- [SecretsManager.5] Rahasia Secrets Manager harus ditandai
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SNS.3] Topik SNS harus ditandai
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.1] Instans Amazon EC2 harus dikelola olehAWS Systems Manager
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik

- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.1]AWS Transfer Familyalur kerja harus diberi tag
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.11]AWS WAFpencatatan ACL web harus diaktifkan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Thailand)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Thailand).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS

- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Athena.2] Katalog data Athena harus ditandai
- [Athena.3] Kelompok kerja Athena harus ditandai
- [Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.2]AWS Backuppoin pemulihan harus ditandai

- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan

- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.1] DataSync tugas harus mengaktifkan logging
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan

- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.172] Pengaturan Akses Publik Blok VPC EC2 harus memblokir lalu lintas gateway internet
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir

- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.182] Blokir pengaturan akses publik harus diaktifkan untuk snapshot Amazon EBS
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [ECS.18] Definisi Tugas ECS harus menggunakan enkripsi dalam transit untuk volume EFS
- [ECS.19] Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi yang dikelola
- [ECS.20] Definisi Tugas ECS harus mengkonfigurasi pengguna non-root dalam definisi wadah Linux

- [ECS.21] Definisi Tugas ECS harus mengkonfigurasi pengguna non-administrator dalam definisi wadah Windows
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis
- [EFS.8] Sistem file EFS harus dienkripsi saat diam
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat

- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.1]AWS Gluepekerjaan harus diberi tag
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat

- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi

- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai

- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik

- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus

- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.38] RDS untuk instans DB PostgreSQL harus dienkripsi saat transit
- [RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit
- [RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch
- [RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB

- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek

- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai

- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.1]AWS Transfer Familyalur kerja harus diberi tag
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan

- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Asia Pasifik (Tokyo)

Kontrol berikut tidak didukung di Wilayah Asia Pasifik (Tokyo).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir

- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Kanada (Pusat)

Kontrol berikut tidak didukung di Wilayah Kanada (Tengah).

- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging

- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus

- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Kanada Barat (Calgary)

Kontrol berikut tidak didukung di Wilayah Kanada Barat (Calgary).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai

- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal

- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.1] DataSync tugas harus mengaktifkan logging
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis

- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan

- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys

- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis
- [EFS.8] Sistem file EFS harus dienkripsi saat diam
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan

- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume

- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil

- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag

- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster

- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node

- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.38] RDS untuk instans DB PostgreSQL harus dienkripsi saat transit
- [RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit
- [RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch
- [RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet

- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok

- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik

- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Tiongkok (Beijing)

Kontrol berikut tidak didukung di Wilayah China (Beijing).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi

- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi
- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi

- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.20] Kedua terowongan VPN untuk AWS Site-to-Site Koneksi VPN harus aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.36] Gateway pelanggan EC2 harus ditandai

- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi

- [ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.23] Penganalisis Akses IAM harus ditandai
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai

- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan

- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.7] Cluster RDS harus mengaktifkan perlindungan penghapusan
- [RDS.12] Otentikasi IAM harus dikonfigurasi untuk cluster RDS
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan
- [RDS.16] Cluster Aurora DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.28] Cluster DB RDS harus diberi tag
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB

- [RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan

- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSOrganisasi saja
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Tiongkok (Ningxia)

Kontrol berikut tidak didukung di Wilayah China (Ningxia).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit

- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi
- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi

- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.20] Kedua terowongan VPN untuk AWS Site-to-Site Koneksi VPN harus aktif
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.36] Gateway pelanggan EC2 harus ditandai
- [EC2.50] Gateway EC2 VPN harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager

- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi
- [ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat

- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat
- [GuardDuty.3] GuardDuty IPset harus ditandai
- [GuardDuty.4] GuardDuty detektor harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.23] Penganalisis Akses IAM harus ditandai

- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik
- [Lambda.2] Fungsi lambda harus menggunakan runtime yang didukung
- [Lambda.3] Fungsi lambda harus dalam VPC

- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.6] Fungsi lambda harus ditandai
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus

- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1

- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat

- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Eropa (Frankfurt)

Kontrol berikut tidak didukung di Wilayah Eropa (Frankfurt).

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai

- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Eropa (Irlandia)

Kontrol berikut tidak didukung di Wilayah Eropa (Irlandia).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus

- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [ECR.4] Repositori publik ECR harus diberi tag
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Eropa (London)

Kontrol berikut tidak didukung di Wilayah Eropa (London).

- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai

- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

Europe (Milan)

Kontrol berikut tidak didukung di Wilayah Eropa (Milan).

- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal

- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [ECR.4] Repositori publik ECR harus diberi tag
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai

- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit

- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [RDS.1] Snapshot RDS harus bersifat pribadi
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer

- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SSM.2] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan patch COMPLIANT setelah instalasi patch
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Eropa (Paris)

Kontrol berikut tidak didukung di Wilayah Eropa (Paris).

- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF

- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai

- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat

- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Eropa (Spanyol)

Kontrol berikut tidak didukung di Wilayah Eropa (Spanyol).

- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi

- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan

- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.1] Snapshot Amazon EBS tidak boleh dikonfigurasi agar dapat dipulihkan secara publik
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan

- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis

- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai

- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.1] Kebijakan fungsi Lambda harus melarang akses publik

- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru

- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus bersifat pribadi
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer

- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Eropa (Stockholm)

Kontrol berikut tidak didukung di Wilayah Eropa (Stockholm).

- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat

- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch

- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai

- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Europe (Zurich)

Kontrol berikut tidak didukung di Wilayah Eropa (Zurich).

- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai

- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai

- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS

- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.4] Repositori publik ECR harus diberi tag

- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan

- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag

- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat

- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus bersifat pribadi
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan

- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan

- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Israel (Tel Aviv)

Kontrol berikut tidak didukung di Wilayah Israel (Tel Aviv).

- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag

- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC

- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan

- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.8] Sistem file EFS harus dienkripsi saat diam
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [ELB.2] Classic Load Balancer dengan SSL/HTTPS pendengar harus menggunakan sertifikat yang disediakan oleh AWS Certificate Manager
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai

- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus

- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai

- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan

- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.1] Snapshot RDS harus bersifat pribadi
- [RDS.4] Snapshot cluster RDS dan snapshot database harus dienkripsi saat diam
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.29] Snapshot cluster RDS DB harus diberi tag
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan

- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Meksiko (Tengah)

Kontrol berikut tidak didukung di Wilayah Meksiko (Tengah).

- [ACM.1] Impor dan ACM-issued sertifikat harus diperpanjang setelah jangka waktu tertentu
- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.4]AWS AppSyncGraphQL API harus diberi tag
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit

- [Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.2]AWS Backuppoin pemulihan harus ditandai
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi

- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CloudTrail.7] Pastikan pencatatan akses bucket S3 diaktifkan pada bucket CloudTrail S3
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.1] URL repositori sumber CodeBuild Bitbucket tidak boleh berisi kredensyal sensitif
- [CodeBuild.2] variabel lingkungan CodeBuild proyek tidak boleh berisi kredensyal teks yang jelas
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai

- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat
- [DataSync.1] DataSync tugas harus mengaktifkan logging
- [DataSync.2] DataSync tugas harus ditandai
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat

- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan
- [DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.34] Tabel rute gateway transit EC2 harus ditandai
- [EC2.40] Gerbang EC2 NAT harus ditandai
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh
- [EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh
- [EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API
- [EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry
- [EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager

- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging
- [EC2.172] Pengaturan Akses Publik Blok VPC EC2 harus memblokir lalu lintas gateway internet
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.182] Blokir pengaturan akses publik harus diaktifkan untuk snapshot Amazon EBS
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer

- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [ECS.18] Definisi Tugas ECS harus menggunakan enkripsi dalam transit untuk volume EFS
- [ECS.19] Penyedia kapasitas ECS harus mengaktifkan perlindungan terminasi yang dikelola
- [ECS.20] Definisi Tugas ECS harus mengkonfigurasi pengguna non-root dalam definisi wadah Linux
- [ECS.21] Definisi Tugas ECS harus mengkonfigurasi pengguna non-administrator dalam definisi wadah Windows
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan
- [EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis
- [EFS.8] Sistem file EFS harus dienkripsi saat diam
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi
- [EKS.7] Konfigurasi penyedia identitas EKS harus diberi tag
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan

- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.3] Domain Elasticsearch harus mengenkripsi data yang dikirim antar node
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [ES.9] Domain Elasticsearch harus diberi tag
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai

- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.1]AWS Gluepekerjaan harus diberi tag
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.1] GuardDuty harus diaktifkan
- [GuardDuty.2] GuardDuty filter harus ditandai
- [GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan
- [GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

- [IAM.7] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.10] Kebijakan kata sandi untuk pengguna IAM harus memiliki konfigurasi yang kuat
- [IAM.11] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf besar
- [IAM.12] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu huruf kecil
- [IAM.13] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu simbol
- [IAM.14] Pastikan kebijakan kata sandi IAM membutuhkan setidaknya satu nomor
- [IAM.15] Pastikan kebijakan kata sandi IAM memerlukan panjang kata sandi minimum 14 atau lebih
- [IAM.16] Pastikan kebijakan kata sandi IAM mencegah penggunaan kembali kata sandi
- [IAM.17] Pastikan kebijakan kata sandi IAM kedaluwarsa kata sandi dalam waktu 90 hari atau kurang
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai

- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoT.4]AWS IoT Coreotorisasi harus diberi tag
- [IoT.5]AWS IoT Corealias peran harus ditandai
- [IoT.6]AWS IoT Corekebijakan harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan

- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch
- [MQ.4] Broker Amazon MQ harus ditandai
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi

- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch
- [RDS.38] RDS untuk instans DB PostgreSQL harus dienkripsi saat transit
- [RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit

- [RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch
- [RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.1] Cluster Amazon Redshift harus melarang akses publik
- [Redshift.2] Koneksi ke cluster Amazon Redshift harus dienkripsi saat transit
- [Redshift.3] Cluster Amazon Redshift harus mengaktifkan snapshot otomatis
- [Redshift.4] Cluster Amazon Redshift harus mengaktifkan pencatatan audit
- [Redshift.6] Amazon Redshift harus mengaktifkan peningkatan otomatis ke versi utama
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.13] Snapshot klaster Redshift harus diberi tag
- [Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi
- [Redshift.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL

- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.7] Bucket tujuan umum S3 harus menggunakan replikasi lintas wilayah
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.22] Bucket tujuan umum S3 harus mencatat peristiwa penulisan tingkat objek
- [S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung

- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [ServiceCatalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.3] Instans Amazon EC2 yang dikelola oleh Systems Manager harus memiliki status kepatuhan asosiasi COMPLIANT
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik

- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Timur Tengah (Bahrain)

Kontrol berikut tidak didukung di Wilayah Timur Tengah (Bahrain).

- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC

- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.10] CloudTrail Penyimpanan data acara danau harus dienkripsi dengan pelanggan yang dikelolaAWS KMS keys
- [CodeArtifact.1] CodeArtifact repositori harus ditandai

- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DocumentDB.6] Cluster Amazon DocumentDB harus dienkripsi saat transit
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.20] Kedua terowongan VPN untuk AWS Site-to-Site Koneksi VPN harus aktif
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys
- [ECS.17] Definisi tugas ECS tidak boleh menggunakan mode jaringan host
- [EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara

- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ
- [FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai

- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [NetworkFirewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.41] RDS untuk instans SQL Server DB harus dienkripsi saat transit
- [RDS.42] RDS untuk instans MariaDB DB harus menerbitkan log ke Log CloudWatch
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.44] RDS untuk instans MariaDB DB harus dienkripsi saat transit
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.4] Ruang nama Redshift Tanpa Server harus dienkripsi dengan pengelolaan pelangganAWS KMS keys
- [RedshiftServerless.5] Ruang nama Redshift Tanpa Server tidak boleh menggunakan nama pengguna admin default
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.8] instance SageMaker notebook harus berjalan pada platform yang didukung
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys

- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Timur Tengah (UAE)

Kontrol berikut tidak didukung di Wilayah Timur Tengah (UEA).

- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit

- [Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFormation.3] CloudFormation tumpukan harus mengaktifkan perlindungan terminasi
- [CloudFormation.4] CloudFormation tumpukan harus memiliki peran layanan terkait
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan

- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudTrail.6] Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [Detective.1] Grafik perilaku Detektif harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.3] Langganan acara DMS harus ditandai
- [DMS.4] Contoh replikasi DMS harus ditandai
- [DMS.5] Grup subnet replikasi DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM
- [DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi
- [DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS
- [DMS.13] Instans replikasi DMS harus dikonfigurasi untuk menggunakan beberapa Availability Zone
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat

- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.4] Instans EC2 yang dihentikan harus dihapus setelah periode waktu tertentu
- [EC2.14] Grup keamanan tidak boleh mengizinkan masuknya dari 0.0.0. 0/0 atau: :/0 ke port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [EC2.180] Antarmuka jaringan EC2 seharusnya mengaktifkan pemeriksaan source/destination
- [EC2.181] Templat peluncuran EC2 harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.183] Koneksi VPN EC2 harus menggunakan protokol IKEv2
- [ECR.4] Repositori publik ECR harus diberi tag
- [EFS.1] Sistem File Elastis harus dikonfigurasi untuk mengenkripsi data file saat istirahat menggunakan AWS KMS
- [EFS.2] Volume Amazon EFS harus dalam rencana cadangan
- [EKS.9] Grup simpul EKS harus berjalan pada versi Kubernetes yang didukung
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomendasikan

- [ELB.18] Pendengar Aplikasi dan Network Load Balancer harus menggunakan protokol aman untuk mengenkripsi data dalam transit
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.1] Node utama klaster EMR Amazon seharusnya tidak memiliki alamat IP publik
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.4]AWS GluePekerjaan percikan harus berjalan pada versi yang didukungAWS Glue
- [GuardDuty.2] GuardDuty filter harus ditandai
- [IAM.1] Kebijakan IAM seharusnya tidak mengizinkan hak administratif “*” penuh
- [IAM.2] Pengguna IAM seharusnya tidak memiliki kebijakan IAM yang dilampirkan
- [IAM.3] Kunci akses pengguna IAM harus diputar setiap 90 hari atau kurang
- [IAM.4] Kunci akses pengguna root IAM seharusnya tidak ada
- [IAM.5] MFA harus diaktifkan untuk semua pengguna IAM yang memiliki kata sandi konsol
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root

- [IAM.8] Kredensi pengguna IAM yang tidak digunakan harus dihapus
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.18] Pastikan peran dukungan telah dibuat untuk mengelola insiden denganAWS Dukungan
- [IAM.19] MFA harus diaktifkan untuk semua pengguna IAM
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.22] Kredensi pengguna IAM yang tidak digunakan selama 45 hari harus dihapus
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess
- [Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan
- [Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai

- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [KMS.1] Kebijakan yang dikelola pelanggan IAM tidak boleh mengizinkan tindakan dekripsi pada semua kunci KMS
- [KMS.2] Prinsipal IAM seharusnya tidak memiliki kebijakan inline IAM yang memungkinkan tindakan dekripsi pada semua kunci KMS
- [Lambda.7] Fungsi lambda harus memiliki AWS X-Ray penelusuran aktif diaktifkan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.4] Kluster MSK harus menonaktifkan akses publik
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [MSK.6] Kluster MSK harus menonaktifkan akses yang tidak diautentikasi
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [Opensearch.9] OpenSearch domain harus ditandai
- [Opensearch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru
- [Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung

- [Redshift.18] Cluster Redshift harus mengaktifkan penerapan Multi-AZ
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer

- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SQS.1] Antrian Amazon SQS harus dienkripsi saat istirahat
- [SQS.2] Antrian SQS harus ditandai
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [SSM.7] Dokumen SSM harus mengaktifkan pengaturan blok berbagi publik
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

Amerika Selatan (Sao Paulo)

Kontrol berikut tidak didukung di Wilayah Amerika Selatan (São Paulo).

- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys

- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir

- [ECR.4] Repositori publik ECR harus diberi tag
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoT.1]AWS IoT Device Defenderprofil keamanan harus ditandai
- [IoT.2]AWS IoT Coretindakan mitigasi harus ditandai
- [IoT.3]AWS IoT Coredimensi harus ditandai
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai

- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan

AWS GovCloud (US-East)

Kontrol berikut tidak didukung di Wil AWS GovCloud (US-East) ayah.

- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi
- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai

- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.4]AWS AppSyncGraphQL API harus diberi tag
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC
- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi

- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus ditandai
- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.2] Kumpulan identitas Cognito seharusnya tidak mengizinkan identitas yang tidak diautentikasi
- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat

- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [Connect.2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan
- [DataSync.2] DataSync tugas harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389
- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.47] Layanan titik akhir Amazon VPC harus diberi tag

- [EC2.52] Gerbang transit EC2 harus ditandai
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root
- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung

- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi
- [ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch
- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara

- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [Glue.3]AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan
- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag

- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM

- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai
- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.31] Grup keamanan RDS DB harus ditandai
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log

- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS
- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.1] Inst SageMaker ans notebook Amazon seharusnya tidak memiliki akses internet langsung
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus

- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.16] SageMaker model harus menggunakan registri pribadi di VPC untuk wadah utama
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SageMaker.19] SageMaker model harus menggunakan registri pribadi di VPC untuk saluran inferensi multi-kontainer
- [SES.1] Daftar kontak SES harus ditandai
- [SES.2] Set konfigurasi SES harus ditandai
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik
- [SSM.5] Dokumen SSM harus ditandai
- [SSM.6] Otomatisasi SSM seharusnya mengaktifkan CloudWatch pencatatan
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging

- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik
- [WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat
- [WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat

AWS GovCloud (US-West)

Kontrol berikut tidak didukung di Wil AWS GovCloud (US-West) ayah.

- [ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- [Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS
- [Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi
- [APIGateway.2] Tahapan API REST API Gateway harus dikonfigurasi untuk menggunakan sertifikat SSL untuk otentikasi backend
- [APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages
- [APIGateway.10] Integrasi API Gateway V2 harus menggunakan HTTPS untuk koneksi pribadi

- [APIGateway.11] Nama domain API Gateway harus menggunakan kebijakan keamanan yang direkomendasikan
- [Amplify.1] Amplify aplikasi harus ditandai
- [Amplify.2] Amplify branch harus diberi tag
- [AppConfig.1]AWS AppConfigaplikasi harus diberi tag
- [AppConfig.2]AWS AppConfigprofil konfigurasi harus ditandai
- [AppConfig.3]AWS AppConfiglingkungan harus ditandai
- [AppConfig.4]AWS AppConfigasosiasi ekstensi harus ditandai
- [AppFlow.1] AppFlow Aliran Amazon harus ditandai
- [AppRunner.1] Layanan Pelari Aplikasi harus ditandai
- [AppRunner.2] Konektor VPC App Runner harus ditandai
- [AppSync.1]AWS AppSyncCache API harus dienkripsi saat istirahat
- [AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan
- [AppSync.4]AWS AppSyncGraphQL API harus diberi tag
- [AppSync.5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API
- [AppSync.6]AWS AppSyncCache API harus dienkripsi saat transit
- [AutoScaling.2] Grup Amazon EC2 Auto Scaling harus mencakup beberapa Availability Zone
- [AutoScaling.3] Konfigurasi peluncuran grup Auto Scaling harus mengonfigurasi instans EC2 agar memerlukan Layanan Metadata Instans Versi 2 (IMDSv2)
- [AutoScaling.6] Grup Auto Scaling harus menggunakan beberapa jenis instance di beberapa Availability Zone
- [AutoScaling.9] Grup Amazon EC2 Auto Scaling harus menggunakan templat peluncuran Amazon EC2
- [Backup.4]AWS Backuprencana laporan harus diberi tag
- [Batch.1] Antrian pekerjaan batch harus ditandai
- [Batch.2] Kebijakan penjadwalan Batch harus ditandai
- [Batch.3] Lingkungan komputasi Batch harus ditandai
- [Batch.4] Properti sumber daya komputasi di lingkungan komputasi Batch terkelola harus ditandai
- [BedrockAgentCore.1] AgentCore Runtime batuan dasar harus dikonfigurasi dengan mode jaringan VPC

- [BedrockAgentCore.2] Bedrock AgentCore Gateways harus memerlukan otorisasi untuk permintaan masuk
- [BedrockAgentCore.3] AgentCore Memori Batuan Dasar harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.4] Bedrock AgentCore Gateway harus dienkripsi dengan pelanggan yang dikelolaAWS KMSkeys
- [BedrockAgentCore.5] Browser AgentCore kustom Bedrock tidak boleh menggunakan mode jaringan publik
- [BedrockAgentCore.6] Browser AgentCore kustom Bedrock harus mengaktifkan perekaman sesi
- [CloudFront.1] CloudFront distribusi harus memiliki objek root default yang dikonfigurasi
- [CloudFront.3] CloudFront distribusi harus memerlukan enkripsi dalam transit
- [CloudFront.4] CloudFront distribusi harus memiliki failover asal yang dikonfigurasi
- Distri CloudFront.5 CloudFront busi [] harus mengaktifkan logging
- [CloudFront.6] CloudFront distribusi harus mengaktifkan WAF
- [CloudFront.7] CloudFront distribusi harus menggunakan SSL/TLS sertifikat khusus
- [CloudFront.8] CloudFront distribusi harus menggunakan SNI untuk melayani permintaan HTTPS
- [CloudFront.9] CloudFront distribusi harus mengenkripsi lalu lintas ke asal khusus
- [CloudFront.10] CloudFront distribusi tidak boleh menggunakan protokol SSL yang tidak digunakan lagi antara lokasi tepi dan asal khusus
- [CloudFront.12] CloudFront distribusi seharusnya tidak menunjuk ke asal S3 yang tidak ada
- [CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal
- [CloudFront.14] CloudFront distribusi harus ditandai
- [CloudFront.15] CloudFront distribusi harus menggunakan kebijakan keamanan TLS yang direkomendasikan
- Distri CloudFront.16 CloudFront busi [] harus menggunakan kontrol akses asal untuk fungsi Lambda URL asal
- Distri CloudFront.17 CloudFront busi harus menggunakan grup kunci tepercaya untuk URL dan cookie yang ditandatangani
- [CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan
- [CodeArtifact.1] CodeArtifact repositori harus ditandai

- [CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [CodeBuild.4] lingkungan CodeBuild proyek harus memiliki loggingAWS Configbuang air kecil
- [CodeGuruProfiler.1] Grup CodeGuru profil profiler harus ditandai
- [CodeGuruReviewer.1] Asosiasi CodeGuru repositori peninjau harus ditandai
- [Cognito.1] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi standar
- [Cognito.3] Kebijakan kata sandi untuk kumpulan pengguna Cognito harus memiliki konfigurasi yang kuat
- [Cognito.4] Kumpulan pengguna Cognito harus mengaktifkan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikasi khusus
- [Cognito.5] MFA harus diaktifkan untuk kumpulan pengguna Cognito
- [Cognito.6] Kumpulan pengguna Cognito harus mengaktifkan perlindungan penghapusan
- [Connect.1] Jenis objek Amazon Connect Customer Profiles harus diberi tag
- [DataSync.2] DataSync tugas harus ditandai
- [DMS.2] Sertifikat DMS harus ditandai
- [DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis
- [DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging
- [DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging
- [DMS.9] Titik akhir DMS harus menggunakan SSL
- [DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat
- [DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai
- [DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik
- [DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch
- [DocumentDB.5] Cluster Amazon DocumentDB harus mengaktifkan perlindungan penghapusan
- [DynamoDB.3] Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- [DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit
- [EC2.21] ACL jaringan seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port 22 atau port 3389

- [EC2.22] Grup keamanan Amazon EC2 yang tidak digunakan harus dihapus
- [EC2.23] Amazon EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- [EC2.24] Jenis instans paravirtual Amazon EC2 tidak boleh digunakan
- [EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [EC2.28] Volume EBS harus dicakup oleh rencana cadangan
- [EC2.38] Instans EC2 harus ditandai
- [EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager
- [EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager Incident Manager
- [EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)
- [EC2.173] Permintaan Armada Spot EC2 dengan parameter peluncuran harus mengaktifkan enkripsi untuk volume EBS terlampir
- [EC2.174] Set opsi EC2 DHCP harus ditandai
- [EC2.175] Templat peluncuran EC2 harus diberi tag
- [EC2.176] Daftar awalan EC2 harus ditandai
- [EC2.177] Sesi cermin lalu lintas EC2 harus ditandai
- [EC2.178] Filter cermin lalu lintas EC2 harus ditandai
- [EC2.179] Target cermin lalu lintas EC2 harus ditandai
- [ECR.1] Repositori pribadi ECR harus memiliki pemindaian gambar yang dikonfigurasi
- [ECR.2] Repositori pribadi ECR harus memiliki kekekalan tag yang dikonfigurasi
- [ECR.3] Repositori ECR harus memiliki setidaknya satu kebijakan siklus hidup yang dikonfigurasi
- [ECR.4] Repositori publik ECR harus diberi tag
- [ECS.3] Definisi tugas ECS tidak boleh membagikan namespace proses host
- [ECS.4] Kontainer ECS harus berjalan sebagai non-istimewa
- [ECS.5] Definisi tugas ECS harus mengonfigurasi wadah agar dibatasi pada akses hanya-baca ke sistem file root

- [ECS.8] Rahasia tidak boleh diteruskan sebagai variabel lingkungan kontainer
- [ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging
- [ECS.10] Layanan ECS Fargate harus berjalan pada versi platform Fargate terbaru
- [ECS.12] Cluster ECS harus menggunakan Wawasan Kontainer
- [EFS.3] Titik akses EFS harus menerapkan direktori root
- [EFS.4] Titik akses EFS harus menegakkan identitas pengguna
- [EKS.2] Cluster EKS harus berjalan pada versi Kubernetes yang didukung
- [EKS.8] Cluster EKS harus mengaktifkan logging audit
- [ELB.10] Classic Load Balancer harus mencakup beberapa Zona Ketersediaan
- [ELB.12] Application Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.13] Penyeimbang Beban Aplikasi, Jaringan, dan Gateway harus menjangkau beberapa Zona Ketersediaan
- [ELB.14] Classic Load Balancer harus dikonfigurasi dengan mode mitigasi desync defensif atau paling ketat
- [ELB.21] Kelompok target Aplikasi dan Network Load Balancer harus menggunakan protokol pemeriksaan kesehatan terenkripsi
- [ELB.22] Kelompok target ELB harus menggunakan protokol transportasi terenkripsi
- [ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis
- [ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis
- [ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis
- [ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat
- [ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan
- [ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH
- [ElastiCache.7] ElastiCache cluster tidak boleh menggunakan grup subnet default
- [ElasticBeanstalk.1] Lingkungan Elastic Beanstalk seharusnya mengaktifkan pelaporan kesehatan yang ditingkatkan
- [ElasticBeanstalk.2] Pembaruan platform yang dikelola Elastic Beanstalk harus diaktifkan
- [ElasticBeanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch

- [EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan
- [EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat
- [EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit
- [ES.4] Pencatatan kesalahan domain Elasticsearch ke CloudWatch Log harus diaktifkan
- [EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- [EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara
- [FraudDetector.1] Jenis entitas Amazon Fraud Detector harus ditandai
- [FraudDetector.2] Label Amazon Fraud Detector harus ditandai
- [FraudDetector.3] Hasil Amazon Fraud Detector harus ditandai
- [FraudDetector.4] Variabel Fraud Detector Amazon harus ditandai
- [FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume
- [FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan
- [GlobalAccelerator.1] Akselerator Global Accelerator harus ditandai
- [GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan
- [GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan
- [GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan
- [GuardDuty.11] GuardDuty Runtime Monitoring harus diaktifkan
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan
- [GuardDuty.13] GuardDuty EC2 Runtime Monitoring harus diaktifkan
- [IAM.6] MFA perangkat keras harus diaktifkan untuk pengguna root
- [IAM.9] MFA harus diaktifkan untuk pengguna root
- [IAM.21] Kebijakan terkelola pelanggan IAM yang Anda buat seharusnya tidak mengizinkan tindakan wildcard untuk layanan
- [IAM.24] Peran IAM harus ditandai
- [IAM.25] Pengguna IAM harus diberi tag
- [IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan
- [Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan

- [IoTSiteWise.1]AWSModel SiteWise aset IoT harus ditandai
- [IoTSiteWise.2]AWS SiteWise Dasbor IoT harus diberi tag
- [IoTSiteWise.3]AWS SiteWise Gateway IoT harus diberi tag
- [IoTSiteWise.4]AWS SiteWise Portal IoT harus diberi tag
- [IoTSiteWise.5]AWS SiteWise Proyek IoT harus diberi tag
- [IoTTwinMaker.1]AWSPekerjaan TwinMaker sinkronisasi IoT harus ditandai
- [IoTTwinMaker.2]AWS TwinMaker Ruang kerja IoT harus diberi tag
- [IoTTwinMaker.3]AWS TwinMaker Adegan IoT harus diberi tag
- [IoTTwinMaker.4]AWS TwinMaker Entitas IoT harus diberi tag
- [IoTWireless.1]AWSGrup multicast Nirkabel IoT harus diberi tag
- [IoTWireless.2]AWSProfil layanan IoT Wireless harus diberi tag
- [IoTWireless.3]AWSTugas IoT FUOTA harus diberi tag
- [IVS.1] Pasangan kunci pemutaran IVS harus ditandai
- [IVS.2] Konfigurasi perekaman IVS harus ditandai
- [IVS.3] Saluran IVS harus ditandai
- [Keyspaces.1] Ruang kunci Amazon Keyspaces harus diberi tag
- [Kinesis.1] Aliran Kinesis harus dienkripsi saat istirahat
- [KMS.5] Kunci KMS tidak boleh diakses publik
- [Lambda.5] Fungsi VPC Lambda harus beroperasi di beberapa Zona Ketersediaan
- [Macie.1] Amazon Macie harus diaktifkan
- [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan
- [MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby
- [MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster
- [MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- [MSK.2] Kluster MSK seharusnya memiliki pemantauan yang ditingkatkan yang dikonfigurasi
- [MSK.3] Konektor MSK Connect harus dienkripsi saat transit
- [MSK.5] Konektor MSK seharusnya mengaktifkan logging
- [Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat

- [Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [Neptune.9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone
- [NetworkFirewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone
- [NetworkFirewall.2] Pencatatan Firewall Jaringan harus diaktifkan
- [NetworkFirewall.3] Kebijakan Network Firewall harus memiliki setidaknya satu kelompok aturan yang terkait
- [NetworkFirewall.4] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket penuh
- [NetworkFirewall.5] Tindakan stateless default untuk kebijakan Network Firewall harus drop atau forward untuk paket yang terfragmentasi
- [NetworkFirewall.6] Grup aturan Stateless Network Firewall tidak boleh kosong
- [NetworkFirewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan
- [Opensearch.1] OpenSearch domain harus mengaktifkan enkripsi saat istirahat
- [Opensearch.2] OpenSearch domain seharusnya tidak dapat diakses publik
- [Opensearch.3] OpenSearch domain harus mengenkripsi data yang dikirim antar node
- [Opensearch.4] login kesalahan OpenSearch domain ke CloudWatch Log harus diaktifkan
- [Opensearch.5] OpenSearch domain harus mengaktifkan pencatatan audit
- [Opensearch.6] OpenSearch domain harus memiliki setidaknya tiga node data
- [Opensearch.7] OpenSearch domain harus mengaktifkan kontrol akses berbutir halus
- [Opensearch.8] Koneksi ke OpenSearch domain harus dienkripsi menggunakan kebijakan keamanan TLS terbaru
- [PCA.1]AWS Private CAotoritas sertifikat root harus dinonaktifkan
- [PCA.2]AWSOtoritas sertifikat CA swasta harus ditandai

- [RDS.14] Cluster Amazon Aurora harus mengaktifkan backtracking
- [RDS.15] Cluster RDS DB harus dikonfigurasi untuk beberapa Zona Ketersediaan
- [RDS.24] Cluster Database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.25] Instans database RDS harus menggunakan nama pengguna administrator khusus
- [RDS.27] Cluster RDS DB harus dienkripsi saat diam
- [RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log
- [RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis
- [RDS.43] Proxy RDS DB harus memerlukan enkripsi TLS untuk koneksi
- [RDS.45] Cluster Aurora MySQL DB harus mengaktifkan logging audit
- [RDS.47] RDS untuk cluster DB PostgreSQL harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.48] RDS untuk cluster MySQL DB harus dikonfigurasi untuk menyalin tag ke snapshot DB
- [RDS.50] Cluster RDS DB harus memiliki cukup periode retensi cadangan yang ditetapkan
- [RDS.51] Cluster global RDS harus berjalan pada versi Aurora MySQL yang didukung
- [Redshift.7] Cluster Redshift harus menggunakan perutean VPC yang ditingkatkan
- [Redshift.8] Cluster Amazon Redshift tidak boleh menggunakan nama pengguna Admin default
- [Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [Redshift.11] Cluster Redshift harus ditandai
- [Redshift.13] Snapshot klaster Redshift harus diberi tag
- [Redshift.17] Grup parameter cluster Redshift harus diberi tag
- [RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan
- [RedshiftServerless.2] Koneksi ke grup kerja Redshift Serverless harus diperlukan untuk menggunakan SSL
- [RedshiftServerless.3] Kelompok kerja Redshift Tanpa Server harus melarang akses publik
- [RedshiftServerless.6] Ruang nama Redshift Tanpa Server harus mengekspor log ke Log CloudWatch
- [Route53.1] Pemeriksaan kesehatan Route 53 harus ditandai
- [Route53.2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS

- [S3.10] Bucket tujuan umum S3 dengan versi diaktifkan harus memiliki konfigurasi Siklus Hidup
- [S3.11] Bucket tujuan umum S3 harus mengaktifkan notifikasi peristiwa
- [S3.12] ACL tidak boleh digunakan untuk mengelola akses pengguna ke bucket tujuan umum S3
- [S3.13] Bucket tujuan umum S3 harus memiliki konfigurasi Siklus Hidup
- [S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA
- [S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok
- [S3.25] Bucket direktori S3 harus memiliki konfigurasi siklus hidup
- [SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook
- [SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.6] konfigurasi gambar SageMaker aplikasi harus diberi tag
- [SageMaker.7] SageMaker gambar harus diberi tag
- [SageMaker.9] definisi pekerjaan kualitas SageMaker data harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.10] definisi pekerjaan penjelasan SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.11] definisi pekerjaan kualitas SageMaker data harus mengaktifkan isolasi jaringan
- [SageMaker.12] definisi pekerjaan bias SageMaker model harus mengaktifkan isolasi jaringan
- [SageMaker.13] definisi pekerjaan kualitas SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.14] jadwal SageMaker pemantauan harus mengaktifkan isolasi jaringan
- [SageMaker.15] definisi pekerjaan bias SageMaker model harus mengaktifkan enkripsi lalu lintas antar kontainer
- [SageMaker.17] toko offline grup SageMaker fitur harus dienkripsi dengan AWS KMS keys
- [SageMaker.18] toko online grup SageMaker fitur dengan penyimpanan standar harus dienkripsi dengan AWS KMS keys
- [SES.3] Set konfigurasi SES harus mengaktifkan TLS untuk mengirim email
- [SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizinkan akses publik
- [SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik
- [SSM.4] Dokumen SSM seharusnya tidak bersifat publik

- [SSM.5] Dokumen SSM harus ditandai
- [StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging
- [StepFunctions.2] Aktivitas Step Functions harus diberi tag
- [Transfer.4] Perjanjian Transfer Family harus ditandai
- [Transfer.5] Sertifikat Transfer Family harus diberi tag
- [Transfer.6] Konektor Transfer Family harus diberi tag
- [Transfer.7] Profil Transfer Family harus diberi tag
- [WAF.1]AWS WAFPencatatan ACL Web Global Klasik harus diaktifkan
- [WAF.2]AWS WAFAturan Regional Klasik harus memiliki setidaknya satu syarat
- [WAF.3]AWS WAFKelompok aturan Regional klasik harus memiliki setidaknya satu aturan
- [WAF.4]AWS WAFACL web Regional Klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.6]AWS WAFAturan global klasik harus memiliki setidaknya satu syarat
- [WAF.7]AWS WAFKelompok aturan global klasik harus memiliki setidaknya satu aturan
- [WAF.8]AWS WAFACL web global klasik harus memiliki setidaknya satu aturan atau grup aturan
- [WAF.10]AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan
- [WAF.12]AWS WAFaturan harus mengaktifkan CloudWatch metrik

Membuat sumber daya CSPM Security Hub dengan CloudFormation

AWSSecurity Hub CSPM terintegrasi denganAWS CloudFormation, yang merupakan layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti aturan otomatisasi), dan CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda.

Bila Anda menggunakanCloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur sumber daya CSPM Security Hub Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

Security Hub CSPM danCloudFormationtemplat

Untuk menyediakan dan mengonfigurasi sumber daya untuk CSPM Security Hub dan layanan terkait, Anda harus memahami cara kerja CloudFormationtemplat. Template adalah file teks dalam format JSON atau YAMM. Template ini menjelaskan sumber daya yang ingin Anda sediakan di CloudFormation tumpukan Anda.

Jika Anda tidak terbiasa dengan JSON atau YAMM, Anda dapat menggunakan CloudFormation Designer untuk membantu Anda memulai dengan template. CloudFormation Untuk informasi lebih lanjut, lihat Apa itu CloudFormation Desainer? dalam AWS CloudFormationUser Guide.

Anda dapat membuat CloudFormation template untuk jenis sumber daya CSPM Security Hub berikut:

- Mengaktifkan Security Hub CSPM
- Menunjuk administrator CSPM Security Hub yang didelegasikan untuk sebuah organisasi
- Tentukan cara organisasi Anda dikonfigurasi di Security Hub CSPM
- Mengaktifkan standar keamanan
- Mengaktifkan agregasi lintas wilayah
- Membuat kebijakan konfigurasi pusat dan mengaitkannya dengan akun, unit organisasi (OU), atau root
- Membuat wawasan khusus
- Membuat aturan otomatisasi
- Menyesuaikan parameter kontrol
- Berlangganan integrasi produk pihak ketiga

Untuk informasi selengkapnya, termasuk contoh template JSON dan YAMAL untuk sumber daya, lihat referensi jenis sumber daya CSPM AWS Security Hub di Panduan Pengguna. AWS CloudFormation

Pelajari lebih lanjut tentangCloudFormation

Untuk mempelajari selengkapnyaCloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormationPanduan Pengguna

- CloudFormationReferensi API
- AWS CloudFormationPanduan Pengguna Antarmuka Baris Perintah

Berlangganan pengumuman CSPM Security Hub dengan Amazon SNS

Bagian ini memberikan informasi tentang berlangganan pengumuman CSPM AWS Security Hub dengan Amazon Simple Notification Service (Amazon SNS) untuk menerima pemberitahuan tentang Security Hub CSPM.

Setelah berlangganan, Anda akan menerima pemberitahuan tentang acara berikut (perhatikan yang sesuai `AnnouncementType` untuk setiap acara):

- `NEW_STANDARDS_CONTROLS`— Kontrol atau standar CSPM Security Hub baru telah ditambahkan.
- `RETIRED_STANDARDS_CONTROLS`— Kontrol atau standar CSPM Security Hub yang ada telah dihentikan.

Notifikasi tersedia dalam semua format yang didukung Amazon SNS. Anda dapat berlangganan pengumuman CSPM Security Hub di semua tempat CSPM Security Wilayah AWS Hub tersedia.

Pengguna harus memiliki `Subscribe` izin untuk berlangganan topik Amazon SNS. Anda dapat mencapai ini dengan kebijakan Amazon SNS, kebijakan IAM, atau keduanya. Untuk informasi selengkapnya, lihat kebijakan IAM dan Amazon SNS bersama-sama di Panduan Pengembang Layanan Pemberitahuan Sederhana Amazon.

> **Note**
>
> Security Hub CSPM mengirimkan pengumuman Amazon SNS tentang pembaruan ke layanan CSPM Security Hub ke semua yang berlangganan. Akun AWS Untuk menerima pemberitahuan tentang temuan CSPM Security Hub, lihat. Meninjau detail dan riwayat temuan di Security Hub CSPM

Anda dapat berlangganan antrian Amazon Simple Queue Service (Amazon SQS) untuk topik Amazon SNS, tetapi Anda harus menggunakan topik Amazon SNS Nama Sumber Daya Amazon (ARN) yang ada di Wilayah yang sama. Untuk informasi selengkapnya, lihat Berlangganan antrian ke topik Amazon SNS di Panduan Pengembang Layanan Antrian Sederhana Amazon.

Anda juga dapat menggunakan AWS Lambda fungsi untuk memanggil acara saat Anda menerima pemberitahuan. Untuk informasi selengkapnya, termasuk kode fungsi contoh, lihat Tutorial: Menggunakan AWS Lambda dengan Amazon Simple Notification Service di Panduan AWS Lambda Pengembang.

ARN topik Amazon SNS untuk setiap Wilayah adalah sebagai berikut.

Wilayah AWS	ARN topik Amazon SNS
AS Timur (Ohio)	`arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements`
AS Timur (Virginia Utara)	`arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements`
AS Barat (California Utara)	`arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements`
AS Barat (Oregon)	`arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`
Afrika (Cape Town)	`arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements`
Asia Pasifik (Hong Kong)	`arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements`
Asia Pasifik (Hyderabad)	`arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
Asia Pasifik (Jakarta)	`arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements`
Asia Pasifik (Mumbai)	`arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements`
Asia Pasifik (Osaka)	`arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements`
Asia Pasifik (Seoul)	`arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements`
Asia Pasifik (Singapura)	`arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements`
Asia Pasifik (Sydney)	`arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements`
Asia Pasifik (Tokyo)	`arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements`
Kanada (Pusat)	`arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements`
Tiongkok (Beijing)	`arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
Tiongkok (Ningxia)	`arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements`
Eropa (Frankfurt)	`arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements`
Eropa (Irlandia)	`arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements`
Eropa (London)	`arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements`
Eropa (Milan)	`arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements`
Eropa (Paris)	`arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements`
Eropa (Spanyol)	`arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements`
Eropa (Stockholm)	`arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements`
Eropa (Zürich)	`arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements`

Wilayah AWS	ARN topik Amazon SNS
Israel (Tel Aviv)	`arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements`
Timur Tengah (Bahrain)	`arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements`
Timur Tengah (UEA)	`arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements`
Amerika Selatan (Sao Paulo)	`arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements`
AWS GovCloud (US-East)	`arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements`
AWS GovCloud (US-West)	`arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements`

Pesan biasanya sama di seluruh Wilayah dalam partisi, sehingga Anda dapat berlangganan satu Wilayah di setiap partisi untuk menerima pengumuman yang memengaruhi semua Wilayah di partisi tersebut. Pengumuman yang terkait dengan akun anggota tidak direplikasi di akun administrator. Akibatnya, setiap akun, termasuk akun administrator, hanya akan memiliki satu salinan dari setiap pengumuman. Anda dapat memutuskan akun mana yang ingin Anda gunakan untuk berlangganan pengumuman CSPM Security Hub.

Untuk informasi tentang biaya berlangganan pengumuman CSPM Security Hub, lihat harga Amazon SNS.

Berlangganan pengumuman CSPM Security Hub (konsol)

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Dalam daftar Wilayah, pilih Wilayah tempat Anda ingin berlangganan pengumuman CSPM Security Hub. Contoh ini menggunakan Wilayah `us-west-2`.
3. Di panel navigasi, pilih Langganan, lalu pilih Buat langganan.
4. Masukkan topik ARN ke dalam topik ARN kotak. Misalnya, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Untuk Protokol, pilih cara Anda ingin menerima pengumuman CSPM Security Hub. Jika Anda memilih Email, untuk Endpoint, masukkan alamat email yang ingin Anda gunakan untuk menerima pengumuman.
6. Pilih Buat langganan.
7. Konfirmasi langganan. Misalnya, jika Anda memilih protokol email, Amazon SNS akan mengirim pesan konfirmasi berlangganan ke email yang Anda berikan.

Berlangganan pengumuman CSPM Security Hub (AWS CLI)

1. Jalankan perintah berikut:

```
 aws  sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-
endpoint your_email@your_domain.com
```

2. Konfirmasi langganan. Misalnya, jika Anda memilih protokol email, Amazon SNS akan mengirim pesan konfirmasi berlangganan ke email yang Anda berikan.

Format pesan Amazon SNS

Contoh berikut menunjukkan pengumuman CSPM Security Hub dari Amazon SNS tentang pengenalan kontrol keamanan baru. Konten pesan bervariasi berdasarkan jenis pengumuman, tetapi formatnya sama untuk semua jenis pengumuman. Secara opsional, `Link` bidang yang memberikan rincian tentang pengumuman dapat disertakan.

Contoh: Pengumuman CSPM Security Hub untuk kontrol baru (protokol email)

```
{
"AnnouncementType":"NEW_STANDARDS_CONTROLS",
```

```
"Title":"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard",
"Description":"We have added 36 new controls to theAWSFoundational Security Best
 Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3,
 AutoScaling.4, AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront
 (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27),
 Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic
 Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon
 Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service
 (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon
 Kinesis (Kinesis.1),AWS Network Firewall(NetworkFirewall.3, NetworkFirewall.4,
 NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift
 (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. "
}
```

Contoh: Pengumuman CSPM Security Hub untuk kontrol baru (protokol Email-JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\":\"NEW_STANDARDS_CONTROLS\",\"Title\":
\"[New Controls] 36 new Security Hub CSPM controls added to theAWSFoundational
 Security Best Practices standard\",\"Description\":\"We have added 36 new
 controls to theAWSFoundational Security Best Practices standard. These
 include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4,
 AutoScaling.6),CloudFormation(CloudFormation.1), Amazon CloudFront (CloudFront.10),
 Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic
 Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service
 (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System
 (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2),
 Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1),AWS
 Network Firewall(NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon
 OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification
 Service (SNS.2),AWS WAF(WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled
 theAWSFoundational Security Best Practices standard in an account and configured
```

```
 Security Hub CSPM to automatically enable new controls, these controls are enabled by
 default. Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
 "HTHgNFRYMetCvisulgLM4CVySvK9qCXFPHQDxYl9tuCFQuIrd7YO4m4YFR28XKMgzqrF20YP
+EilipUm2SOTpEEtOTekU5bn74+YmNZfwr4aPFx0vUuQCVOshmHl37hjkiLjhCg/t53QQiLfP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUsOG8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRWcjDwqTXz5nR6Ywv1ZqZfLIl7gYKslt+jsyd/k+7kOqGmOJRDr7qhE7H
+7vaGRLOptsQnbW8VmeYnDbahEO8FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```


Menonaktifkan CSPM Security Hub

Anda dapat menonaktifkan CSPM AWS Security Hub dengan menggunakan konsol CSPM Security Hub atau Security Hub API. Jika Anda menonaktifkan Security Hub CSPM, Anda dapat mengaktifkannya lagi nanti.

Jika organisasi Anda menggunakan konfigurasi pusat, administrator CSPM Security Hub yang didelegasikan dapat membuat kebijakan konfigurasi yang menonaktifkan CSPM Security Hub untuk akun tertentu dan unit organisasi (OU) dan tetap mengaktifkan CSPM Security Hub untuk orang lain. Kebijakan konfigurasi memengaruhi Wilayah asal dan semua Wilayah yang ditautkan. Untuk informasi selengkapnya, lihat Memahami konfigurasi pusat di Security Hub CSPM.

Jika Anda menonaktifkan CSPM Security Hub untuk sebuah akun, hal berikut akan terjadi:

- Semua standar dan kontrol CSPM Security Hub dinonaktifkan untuk akun.
- Security Hub CSPM berhenti menghasilkan, memperbarui, dan menelan temuan untuk akun tersebut.
- Setelah 30 hari, Security Hub CSPM secara permanen menghapus semua temuan arsip yang ada untuk akun tersebut. Temuan ini tidak dapat dipulihkan dengan menggunakan Security Hub CSPM.
- Setelah 90 hari, Security Hub CSPM secara permanen menghapus semua temuan aktif yang ada untuk akun tersebut. Temuan ini tidak dapat dipulihkan dengan menggunakan Security Hub CSPM.

- Setelah 90 hari, Security Hub CSPM secara permanen menghapus semua wawasan yang ada dan pengaturan konfigurasi CSPM Security Hub untuk akun tersebut. Data dan pengaturan tidak dapat dipulihkan.

Untuk mempertahankan temuan yang ada, Anda dapat mengekspor temuan ke bucket S3 sebelum menonaktifkan CSPM Security Hub. Anda dapat melakukan ini dengan menggunakan tindakan kustom dengan EventBridge aturan Amazon. Untuk informasi selengkapnya, lihat Menggunakan EventBridge untuk respon otomatis dan remediasi.

Jika Anda mengaktifkan kembali CSPM Security Hub dalam waktu 90 hari setelah menonaktifkannya untuk akun, Anda mendapatkan kembali akses ke temuan aktif yang ada, serta wawasan dan pengaturan konfigurasi CSPM Security Hub untuk akun tersebut. Jika Anda mengaktifkan kembali CSPM Security Hub dalam waktu 30 hari, Anda juga mendapatkan kembali akses ke temuan arsip yang ada untuk akun tersebut. Namun, temuan yang ada mungkin tidak akurat karena akan mencerminkan keadaan AWS lingkungan Anda saat Anda menonaktifkan CSPM Security Hub. Selain itu, saat Anda mengaktifkan kembali standar dan kontrol individual, Security Hub CSPM mungkin awalnya menghasilkan temuan duplikat untuk AWS sumber daya tertentu, tergantung pada standar dan kontrol yang Anda aktifkan. Untuk alasan ini, kami menyarankan Anda melakukan salah satu hal berikut:

- Ubah status alur kerja dari semua temuan yang ada `RESOLVED` sebelum Anda menonaktifkan CSPM Security Hub. Untuk informasi selengkapnya, lihat Mengatur status alur kerja temuan.
- Nonaktifkan semua standar setidaknya enam hari sebelum Anda menonaktifkan Security Hub CSPM. Security Hub CSPM kemudian mengarsipkan semua temuan yang ada berdasarkan upaya terbaik, biasanya dalam waktu tiga hingga lima hari. Untuk informasi selengkapnya, lihat Menonaktifkan standar.

Anda tidak dapat menonaktifkan CSPM Security Hub dalam kasus berikut:

- Akun Anda adalah akun administrator CSPM Security Hub yang didelegasikan untuk organisasi. Jika Anda menggunakan konfigurasi pusat, Anda tidak dapat mengaitkan kebijakan konfigurasi yang menonaktifkan CSPM Security Hub untuk akun administrator yang didelegasikan. Asosiasi dapat berhasil untuk akun lain, tetapi CSPM Security Hub tidak menerapkan kebijakan tersebut ke akun administrator yang didelegasikan.
- Akun Anda adalah akun administrator CSPM Security Hub berdasarkan undangan, dan Anda memiliki akun anggota. Sebelum Anda dapat menonaktifkan Security Hub CSPM, Anda harus

memisahkan semua akun anggota Anda. Untuk mempelajari caranya, lihat the section called "Memutuskan akun anggota".

Sebelum pemilik akun anggota dapat menonaktifkan CSPM Security Hub, akun tersebut harus memisahkan diri dari akun administratornya. Untuk akun organisasi, hanya akun administrator yang dapat memisahkan akun anggota. Untuk informasi selengkapnya, lihat the section called "Memutuskan akun anggota organisasi". Untuk akun yang diundang secara manual, akun administrator atau akun anggota dapat memisahkan akun. Untuk informasi selengkapnya, lihat the section called "Memutuskan akun anggota" atau the section called "Memutuskan hubungan dari akun administrator". Pemutusan tidak diperlukan jika Anda menggunakan konfigurasi pusat karena administrator CSPM Security Hub dapat membuat kebijakan yang menonaktifkan CSPM Security Hub untuk akun anggota tertentu.

Saat Anda menonaktifkan CSPM Security Hub untuk sebuah akun, CSPM hanya dinonaktifkan saat ini. Wilayah AWS Namun, jika Anda menggunakan konfigurasi pusat untuk menonaktifkan CSPM Security Hub untuk akun tertentu, itu dinonaktifkan di Wilayah beranda dan semua Wilayah yang ditautkan.

Untuk menonaktifkan CSPM Security Hub, pilih metode pilihan Anda dan ikuti langkah-langkahnya.

Security Hub CSPM console

Ikuti langkah-langkah ini untuk menonaktifkan CSPM Security Hub dengan menggunakan konsol.

Untuk menonaktifkan CSPM Security Hub

1. Buka konsol CSPM AWS Security Hub di. https://console.aws.amazon.com/securityhub/
2. Di panel navigasi, pada Pengaturan, pilih Umum.
3. Di bagian Nonaktifkan CSPM Security Hub, pilih Nonaktifkan CSPM Security Hub.
4. Saat diminta konfirmasi, pilih Nonaktifkan CSPM Security Hub.

Security Hub API

Untuk menonaktifkan Security Hub CSPM secara terprogram, gunakan DisableSecurityHubpengoperasian Security Hub AWS API. Atau, jika Anda menggunakanAWS CLI, jalankan perintah disable-security-hub. Misalnya, perintah berikut menonaktifkan CSPM Security Hub saat ini: Wilayah AWS

```
$ aws securityhub disable-security-hub
```

Keamanan di AWS Security Hub CSPM

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama AWS antara Anda. Model tanggung jawab bersama menggambarkan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Third-partyauditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari program AWS kepatuhan. Untuk mempelajari program kepatuhan yang berlaku di AWS Security Hub CSPM, lihat Cakupan Layanan Menurut Program Kepatuhan AWS.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Security Hub CSPM. Topik berikut menunjukkan cara mengonfigurasi Security Hub CSPM untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya CSPM Security Hub Anda.

Topik

- Perlindungan data di AWS Security Hub CSPM
- AWS Identitas dan Manajemen Akses untuk Security Hub CSPM
- Validasi kepatuhan untuk AWS Security Hub CSPM
- Ketahanan di AWS Hub Keamanan
- Keamanan infrastruktur di AWS Security Hub CSPM
- AWS Security Hub CSPM dan antarmuka titik akhir VPC (AWS PrivateLink)

Perlindungan data di AWS Security Hub CSPM

Model tanggung jawab bersama AWS berlaku untuk perlindungan data di AWS Security Hub CSPM. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data Ket . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredenSIAL dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di Panduan AWS CloudTrail Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Security Hub CSPM atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat

menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Security Hub CSPM adalah penawaran layanan multi-tenant. Untuk memastikan perlindungan data, Security Hub CSPM mengenkripsi data saat istirahat dan data dalam transit antar layanan komponen.

AWS Identitas dan Manajemen Akses untuk Security Hub CSPM

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan di otorisasi (memiliki izin) untuk menggunakan sumber daya Hub Keamanan. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Cara kerja Security Hub dengan IAM
- Identity-based Contoh kebijakan untuk AWS Security Hub CSPM
- Service-linked peran untuk AWS Security Hub CSPM
- AWS kebijakan terkelola untuk Security Hub
- Pemecahan masalah AWS Security Hub CSPM Identitas dan Akses

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat Pemecahan masalah AWS Security Hub CSPM Identitas dan Akses)
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat Cara kerja Security Hub dengan IAM)
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat Identity-based Contoh kebijakan untuk AWS Security Hub CSPM)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredentif identitas Anda. Anda harus diautentikasi sebagai Pengguna root akun AWS, pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk sebagai identitas federasi menggunakan kredenSIAL dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), otentikasi masuk tunggal, atau kredenSIAL. Google/ Facebook Untuk informasi selengkapnya tentang cara masuk, lihat Cara masuk ke Akun AWS Anda dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS menyediakan SDK dan CLI untuk menandatangani permintaan kriptografis. Untuk informasi selengkapnya, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredenSIAL sementara.

Identi tas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredenSIAL dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat Apa itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat Memerlukan pengguna manusia untuk menggunakan federasi dengan

penyedia identitas untuk mengakses AWS menggunakan kredenSIAL sementara di Panduan Pengguna IAM.

Grup IAM menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan beralih dari pengguna ke peran IAM (konsol) atau dengan memanggil operasi AWS CLI AWS API. Untuk informasi selengkapnya, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Identity-based kebijakan

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan dalam Panduan Pengguna IAM.

Identity-based kebijakan dapat berupa kebijakan sebaris (disematkan langsung ke dalam satu identitas) atau kebijakan ter kelola (kebijakan mandiri yang dilampirkan ke beberapa identitas). Untuk mempelajari cara memilih antara kebijakan terkelola dan kebijakan inline, lihat Pilih antara kebijakan terkelola dan kebijakan inline dalam Panduan Pengguna IAM.

Resource-based kebijakan

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus menentukan principal dalam kebijakan berbasis sumber daya.

Resource-based kebijakan adalah kebijakan sebaris yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat mengatur izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – Menentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCP) – Menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat Kebijakan kontrol sumber daya (RCP) dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Cara kerja Security Hub dengan IAM

Sebelum Anda menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses ke AWS Security Hub CSPM, pelajari fitur IAM mana yang tersedia untuk digunakan dengan Security Hub CSPM.

Fitur IAM yang dapat Anda gunakan AWS Security Hub CSPM

Fitur IAM	Dukungan CSPM Hub Keamanan
Identity-based kebijakan	Ya
Resource-based kebijakan	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Tidak
Kunci kondisi kebijakan	Ya
Daftar kontrol akses (ACL)	Tidak
Attribute-based kontrol akses (ABAC) - tag dalam kebijakan	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Service-linked peran	Ya

Untuk tampilan tingkat tinggi tentang cara kerja Security Hub CSPM dan lainnya dengan Layanan AWS sebagian besar fitur IAM, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

Identity-based kebijakan untuk Security Hub CSPM

Mendukung kebijakan berbasis identitas: Ya

Identity-based kebijakan adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Security Hub CSPM mendukung kebijakan berbasis identitas. Untuk informasi selengkapnya, lihat Identity-based Contoh kebijakan untuk AWS Security Hub CSPM.

Resource-based kebijakan untuk Security Hub CSPM

Mendukung kebijakan berbasis sumber daya: Tidak

Resource-based kebijakan adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh principal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai principal dalam kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Security Hub CSPM tidak mendukung kebijakan berbasis sumber daya. Anda tidak dapat melampirkan kebijakan IAM secara langsung ke sumber daya CSPM Security Hub.

Tindakan kebijakan untuk Security Hub CSPM

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Security Hub CSPM menggunakan awalan berikut sebelum tindakan:

```
securityhub:
```

Misalnya, untuk memberikan izin pengguna untuk mengaktifkan CSPM Hub Keamanan, yang merupakan tindakan yang sesuai dengan pen `EnableSecurityHub` goperasian API CSPM Hub Keamanan, sertakan `securityhub:EnableSecurityHub` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Security Hub CSPM mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

```
"Action": "securityhub:EnableSecurityHub"
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma. Contoh:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Sebagai contoh, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut:

```
"Action": "securityhub:Get*"
```

Namun, sebagai praktik terbaik, Anda harus membuat kebijakan yang mengikuti prinsip hak istimewa paling sedikit. Dengan kata lain, Anda harus membuat kebijakan yang hanya menyertakan izin yang diperlukan untuk melakukan tugas tertentu.

Pengguna harus memiliki akses ke `DescribeStandardsControl` operasi untuk memiliki akses ke`BatchGetSecurityControls`,`BatchGetStandardsControlAssociations`, dan`ListStandardsControlAssociations`.

Pengguna harus memiliki akses ke `UpdateStandardsControls` operasi untuk memiliki akses ke`BatchUpdateStandardsControlAssociations`, dan`UpdateSecurityControl`.

Untuk daftar tindakan CSPM Security Hub, lihat Tindakan yang ditentukan oleh AWS Security Hub CSPM dalam Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan tindakan CSPM Security Hub, lihat. Identity-based Contoh kebijakan untuk AWS Security Hub CSPM

Sumber daya kebijakan untuk Security Hub CSPM

Mendukung sumber daya kebijakan: Tidak

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Security Hub CSPM mendefinisikan jenis sumber daya berikut:

- Hub
- Produk
- Menemukan agregator, juga disebut sebagai agregator lintas wilayah
- Aturan otomatisasi
- Kebijakan konfigurasi

Anda dapat menentukan jenis sumber daya ini dalam kebijakan dengan menggunakan ARN.

Untuk daftar jenis sumber daya CSPM Security Hub dan sintaks ARN untuk masing-masing, lihat Jenis sumber daya yang ditentukan oleh AWS Security Hub CSPM dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan untuk setiap jenis sumber daya, lihat Tind akan yang ditentukan oleh AWS Security Hub CSPM dalam Referensi Otorisasi Layanan. Untuk contoh kebijakan yang menentukan sumber daya, lihatIdentity-based Contoh kebijakan untuk AWS Security Hub CSPM.

Kunci kondisi kebijakan untuk Security Hub CSPM

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM.

Untuk daftar kunci kondisi CSPM Hub Keamanan, lihat Kunci kondisi untuk AWS Security Hub CSPM di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya mana yang dapat digunakan dengan kunci kondisi, lihat Tind akan yang ditentukan oleh AWS Security Hub CSPM. Untuk contoh kebijakan yang menggunakan kunci kondisi, lihatIdentity-based Contoh kebijakan untuk AWS Security Hub CSPM.

Daftar kontrol akses (ACL) di Security Hub CSPM

Mendukung ACL: Tidak

Daftar kontrol akses (ACL) mengendalikan principal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Security Hub CSPM tidak mendukung ACL, yang berarti Anda tidak dapat melampirkan ACL ke sumber daya CSPM Security Hub.

Attribute-based kontrol akses (ABAC) dengan Security Hub CSPM

Mendukung ABAC (tanda dalam kebijakan): Ya

Attribute-based kontrol akses (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut yang disebut tag. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi ketika tag kepala sekolah cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Anda dapat melampirkan tag ke sumber daya CSPM Security Hub. Anda juga dapat mengontrol akses ke sumber daya dengan memberikan informasi tag di `Condition` elemen kebijakan.

Untuk informasi tentang menandai sumber daya CSPM Security Hub, lihat. Menandai sumber daya Security Hub Untuk contoh kebijakan berbasis identitas yang mengontrol akses ke sumber daya berdasarkan tag, lihat. Identity-based Contoh kebijakan untuk AWS Security Hub CSPM

Menggunakan kredenSIAL sementara dengan Security Hub CSPM

Mendukung kredensial sementara: Ya

KredenSIAL sementara menyediakan akses jangka pendek ke AWS sumber daya dan dibuat secara otomatis saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis membuat kredenSIAL sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM dan Layanan AWS yang berfungsi dengan IAM dalam Panduan Pengguna IAM.

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda mendapatkan kredentif keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRole atau GetFederationToken.

Security Hub CSPM mendukung penggunaan kredenSIAL sementara.

Teruskan sesi akses untuk Security Hub CSPM

Mendukung sesi akses terusan (FAS): Ya

Sesi akses maju (FAS) menggunakan izin dari kepala sekolah yang memanggil Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses terusan.

Misalnya, Security Hub CSPM membuat permintaan FAS ke hilir Layanan AWS saat Anda mengintegrasikan Security Hub CSPM dengan AWS Organizations dan ketika Anda menetapkan akun administrator CSPM Hub Keamanan yang didelegasikan untuk organisasi di Organisasi.

Untuk tugas lain, Security Hub CSPM menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihatService-linked peran untuk AWS Security Hub CSPM.

Peran layanan untuk Security Hub CSPM

Security Hub CSPM tidak mengambil atau menggunakan peran layanan. Untuk melakukan tindakan atas nama Anda, Security Hub CSPM menggunakan peran terkait layanan. Untuk detail tentang peran ini, lihatService-linked peran untuk AWS Security Hub CSPM.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat menimbulkan masalah operasional dengan penggunaan CSPM Hub Keamanan Anda. Edit peran layanan hanya jika Security Hub CSPM memberikan panduan untuk melakukannya.

Service-linked peran untuk Security Hub CSPM

Mendukung peran terkait layanan: Ya

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan dapat mengambil peran untuk melakukan tindakan atas nama Anda. Service-linked peran muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Security Hub CSPM menggunakan peran terkait layanan untuk melakukan tindakan atas nama Anda. Untuk detail tentang peran ini, lihatService-linked peran untuk AWS Security Hub CSPM.

Identity-based Contoh kebijakan untuk AWS Security Hub CSPM

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya CSPM Security Hub. Mereka juga tidak dapat melakukan tugas menggunakan Konsol Manajemen AWS, AWS CLI, atau AWS API. Administrator harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol CSPM Security Hub
- Contoh: Izinkan pengguna untuk melihat izin mereka sendiri
- Contoh: Mengizinkan pengguna membuat dan mengelola kebijakan konfigurasi
- Contoh: Izinkan pengguna untuk melihat temuan
- Contoh: Izinkan pengguna membuat dan mengelola aturan otomatisasi

Praktik terbaik kebijakan

Identity-based kebijakan menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Hub Keamanan di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai kebijakan AWS terkelola dan beralih ke izin hak istimewa terendah — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkel AWS ola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui tindakan tertentu Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang memerlukan pengguna IAM atau pengguna root Akun AWS, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

Menggunakan konsol CSPM Security Hub

Untuk mengakses AWS Security Hub CSPM konsol, Anda harus memiliki seperangkat izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya CSPM Hub Keamanan di situs Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

Untuk memastikan bahwa pengguna dan peran tersebut dapat menggunakan konsol CSPM Security Hub, lampirkan juga kebijakan terkel AWS ola berikut ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
```

```
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Contoh: Izinkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau secara terprogram menggunakan API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
```

```
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Mengizinkan pengguna membuat dan mengelola kebijakan konfigurasi

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan IAM yang memungkinkan pengguna membuat, melihat, memperbarui, dan menghapus kebijakan konfigurasi. Kebijakan contoh ini juga memungkinkan pengguna untuk memulai, menghentikan, dan melihat asosiasi kebijakan. Agar kebijakan IAM ini berfungsi, pengguna harus menjadi administrator CSPM Hub Keamanan yang didelegasikan untuk suatu organisasi.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateConfigurationPolicy",
                "securityhub:UpdateConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetConfigurationPolicy",
                "securityhub:ListConfigurationPolicies"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "DeleteConfigurationPolicy",
            "Effect": "Allow",
            "Action": [
                "securityhub:DeleteConfigurationPolicy"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetConfigurationPolicyAssociations",
                "securityhub:GetConfigurationPolicyAssociation",
                "securityhub:ListConfigurationPolicyAssociations"
            ],
            "Resource": "*"
        },
        {
            "Sid": "UpdateConfigurationPolicyAssociation",
            "Effect": "Allow",
            "Action": [
                "securityhub:StartConfigurationPolicyAssociation",
                "securityhub:StartConfigurationPolicyDisassociation"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan pengguna untuk melihat temuan

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan IAM yang memungkinkan pengguna untuk melihat temuan CSPM Hub Keamanan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh: Izinkan pengguna membuat dan mengelola aturan otomatisasi

Contoh ini menunjukkan bagaimana Anda dapat membuat kebijakan IAM yang memungkinkan pengguna membuat, melihat, memperbarui, dan menghapus aturan otomatisasi CSPM Security Hub. Agar kebijakan IAM ini berfungsi, pengguna harus menjadi administrator CSPM Hub Keamanan. Untuk membatasi izin — misalnya, untuk mengizinkan pengguna hanya melihat aturan otomatisasi — Anda dapat menghapus izin buat, perbarui, dan hapus.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateAndUpdateAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:CreateAutomationRule",
                "securityhub:BatchUpdateAutomationRules"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ViewAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchGetAutomationRules",
                "securityhub:ListAutomationRules"
            ],
            "Resource": "*"
```

```
        },
        {
            "Sid": "DeleteAutomationRules",
            "Effect": "Allow",
            "Action": [
                "securityhub:BatchDeleteAutomationRules"
            ],
            "Resource": "*"
        }
    ]
}
```

Service-linked peran untuk AWS Security Hub CSPM

AWS Security Hub CSPM menggunakan peran terkait layanan AWS Identity and Access Management (IAM) bernama. `AWSServiceRoleForSecurityHub` Peran terkait layanan ini adalah peran IAM yang ditautkan langsung ke Security Hub CSPM. Ini telah ditentukan sebelumnya oleh Security Hub CSPM, dan mencakup semua izin yang diperlukan Security Hub CSPM untuk memanggil AWS sumber daya lain Layanan AWS dan memantau atas nama Anda. Security Hub CSPM menggunakan peran terkait layanan ini di semua Wilayah AWS tempat CSPM Security Hub tersedia.

Peran terkait layanan membuat pengaturan Security Hub CSPM lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Security Hub CSPM mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Security Hub CSPM yang dapat mengambil peran tersebut. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan Anda tidak dapat melampirkan kebijakan izin tersebut ke entitas IAM lainnya.

Untuk meninjau detail peran terkait layanan, Anda dapat menggunakan konsol CSPM Security Hub. Di panel navigasi, pilih Umum di bawah Peng aturan. Kemudian, di bagian Izin layanan, pilih Lihat izin layanan.

Anda dapat menghapus peran terkait layanan Security Hub CSPM hanya setelah menonaktifkan Security Hub CSPM di semua Wilayah yang diaktifkan. Ini melindungi sumber daya CSPM Security Hub Anda karena Anda tidak dapat menghapus izin untuk mengaksesnya secara tidak sengaja.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM dan cari layanan yang memiliki Ya di kolom peran. Service-linked Pilih Ya dengan tautan untuk meninjau dokumentasi peran terkait layanan untuk layanan tersebut.

Topik

- Service-linked izin peran untuk Security Hub CSPM
- Membuat peran terkait layanan untuk Security Hub CSPM
- Mengedit peran terkait layanan untuk Security Hub CSPM
- Menghapus peran terkait layanan untuk Security Hub CSPM

Service-linked izin peran untuk Security Hub CSPM

Security Hub CSPM menggunakan peran terkait layanan bernama. `AWSServiceRoleForSecurityHub` Ini adalah peran terkait layanan yang diperlukan AWS Security Hub CSPM untuk mengakses sumber daya Anda. Peran terkait layanan ini memungkinkan Security Hub CSPM untuk melakukan tugas seperti menerima temuan dari orang lain Layanan AWS dan mengonfigurasi AWS Config infrastruktur yang diperlukan untuk menjalankan pemeriksaan keamanan untuk kontrol. Peran terkait layanan `AWSServiceRoleForSecurityHub` memercayai layanan `securityhub.amazonaws.com` untuk menjalankan peran.

Per `AWSServiceRoleForSecurityHub` an terkait layanan menggunakan kebijakan terkelola. `AWSSecurityHubServiceRolePolicy`

Anda harus memberikan izin untuk mengizinkan identitas IAM (seperti peran, grup, atau pengguna) untuk membuat, mengedit, atau menghapus peran terkait layanan. Agar peran `AWSServiceRoleForSecurityHub` terkait layanan berhasil dibuat, identitas IAM yang Anda gunakan untuk mengakses CSPM Hub Keamanan harus memiliki izin yang diperlukan. Untuk memberikan izin yang diperlukan, lampirkan kebijakan berikut untuk identitas IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Membuat peran terkait layanan untuk Security Hub CSPM

Per `AWSServiceRoleForSecurityHub` an tertaut layanan dibuat secara otomatis saat Anda mengaktifkan CSPM Hub Keamanan untuk pertama kalinya atau Anda mengaktifkan CSPM Hub Keamanan di Wilayah yang sebelumnya tidak Anda aktifkan. Anda juga dapat membuat peran `AWSServiceRoleForSecurityHub` terkait layanan secara manual menggunakan konsol IAM, IAM CLI, atau IAM API. Untuk informasi selengkapnya tentang membuat peran secara manual, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM.

> **Important**
>
> Peran terkait layanan yang dibuat untuk akun administrator CSPM Security Hub tidak berlaku untuk akun anggota CSPM Security Hub terkait.

Mengedit peran terkait layanan untuk Security Hub CSPM

Security Hub CSPM tidak mengizinkan Anda mengedit peran terkait layanan`AWSServiceRoleForSecurityHub`. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengubah deskripsi peran dengan menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Security Hub CSPM

Jika Anda tidak lagi perlu menggunakan sebuah fitur atau layanan yang memerlukan sebuah peran terkait layanan, kami merekomendasikan Anda untuk menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif.

Saat Anda menonaktifkan Security Hub CSPM, Security Hub CSPM tidak secara otomatis menghapus peran terkait layanan untuk Anda`AWSServiceRoleForSecurityHub`. Jika Anda mengaktifkan CSPM Security Hub lagi, layanan kemudian dapat mulai menggunakan peran terkait layanan yang ada lagi. Jika Anda tidak perlu lagi menggunakan Security Hub CSPM, Anda dapat menghapus peran terkait layanan secara manual.

> **Important**
>
> Sebelum menghapus peran yang dit `AWSServiceRoleForSecurityHub` autkan layanan, Anda harus terlebih dahulu menonaktifkan Security Hub CSPM di semua Wilayah tempat peran tersebut diaktifkan. Untuk informasi selengkapnya, lihat Menonaktifkan CSPM Security Hub. Jika Security Hub CSPM tidak dinonaktifkan saat Anda mencoba menghapus peran terkait layanan, penghapusan gagal.

Untuk menghapus peran `AWSServiceRoleForSecurityHub` terkait layanan, Anda dapat menggunakan konsol IAM, IAM CLI, atau IAM API. Untuk informasi selengkapnya, lihat Menghapus peran terkait layanan dalam Panduan Pengguna IAM.

AWS kebijakan terkelola untuk Security Hub

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan ter AWS kelola mungkin tidak memberikan izin hak istimewa terkecil untuk kasus penggunaan spesifik Anda karena kebijakan tersebut tersedia untuk digunakan semua AWS pelanggan. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan ter AWS kelola ketika yang baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat Kebijakan terkelola AWS dalam Panduan Pengguna IAM.

AWS kebijakan yang dikelola: AWSSecurityHubFullAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan CSPM Hub Keamanan. Kebijakan ini harus dilampirkan ke prinsipal sebelum mereka mengaktifkan Security Hub CSPM secara manual untuk akun mereka. Misalnya, kepala sekolah dengan izin ini dapat melihat dan memperbarui status temuan. Mereka juga dapat mengonfigurasi wawasan khusus, mengaktifkan integrasi, dan mengaktifkan serta menonaktifkan standar dan kontrol. Prinsipal untuk akun administrator juga dapat mengelola akun anggota.

Detail izin

Kebijakan ini mencakup izin berikut:

- `securityhub`- Memungkinkan kepala sekolah akses penuh ke semua tindakan CSPM Hub Keamanan.
- `guardduty`— Memungkinkan kepala sekolah melakukan manajemen siklus hidup penuh detektor, manajemen admin organisasi, pengelolaan akun anggota, dan konfigurasi seluruh organisasi di Amazon. GuardDuty Ini termasuk tindakan API: GetDetector, ListDetector CreateDetector, UpdateDetector, DeleteDetector, EnableOrganizationAdminAccount, ListOrganizationAdminAccounts, CreateMembers, UpdateOrganizationConfiguration, DescribeOrganizationConfiguration.
- `iam`- Memungkinkan prinsipal untuk membuat peran terkait layanan untuk Security Hub CSPM dan Security Hub dan untuk mendapatkan peran, kebijakan, dan versi kebijakan.
- `inspector`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang status akun, mengaktifkan atau menonaktifkan, mendelegasikan manajemen admin, dan melakukan manajemen konfigurasi organisasi di Amazon Inspector. Ini termasuk tindakan API: BatchGetAccountStatus, Aktifkan, Nonaktifkan EnableDelegatedAdminAccount, DisableDelegatedAdminAccount, ListDelegatedAdminAccounts,, UpdateOrganizationConfiguration, DescribeOrganizationConfiguration.
- `pricing`— Memungkinkan prinsipal untuk mendapatkan daftar harga Layanan AWS dan produk.
- `account`— Memungkinkan kepala sekolah untuk mendapatkan informasi tentang Wilayah akun untuk mendukung manajemen Wilayah di Hub Keamanan.

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubFullAccess di Panduan Referensi AWS Kebijakan Terkelola.

AWS kebijakan yang dikelola: AWSSecurityHubReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin baca-saja yang memungkinkan pengguna melihat informasi di Security Hub CSPM. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Security Hub CSPM. Misalnya, kepala sekolah dengan izin ini dapat melihat daftar temuan yang terkait dengan akun mereka, tetapi tidak dapat mengubah status temuan. Mereka dapat melihat hasil wawasan, tetapi tidak dapat membuat atau mengonfigurasi wawasan khusus. Mereka tidak dapat mengonfigurasi kontrol atau integrasi produk.

Detail izin

Kebijakan ini mencakup izin berikut:

- `securityhub`— Memungkinkan pengguna untuk melakukan tindakan yang mengembalikan daftar item atau detail tentang item. Ini termasuk operasi API yang dimulai dengan`Get`,`List`, atau`Describe`.

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubReadOnlyAccess di Panduan Referensi AWS Kebijakan Terkelola.

AWS kebijakan yang dikelola: AWSSecurityHubOrganizationsAccess

Anda dapat melampirkan kebijakan `AWSSecurityHubOrganizationsAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif untuk mengaktifkan dan mengelola Security Hub, Security Hub CSPM, Amazon, GuardDuty dan Amazon Inspector untuk organisasi di. AWS Organizations Izin untuk kebijakan ini memungkinkan akun manajemen organisasi untuk menetapkan akun administrator yang didelegasikan untuk Security Hub, Security Hub CSPM, Amazon, GuardDuty dan Amazon Inspector. Mereka juga mengizinkan akun administrator yang didelegasikan untuk mengaktifkan akun organisasi sebagai akun anggota.

Kebijakan ini hanya memberikan izin untuk AWS Organizations. Akun manajemen organisasi dan akun administrator yang didelegasikan juga memerlukan izin untuk tindakan terkait. Izin ini dapat diberikan menggunakan kebijakan ter `AWSSecurityHubFullAccess` kelola.

Membuat atau memperbarui kebijakan administrator yang didelegasikan di akun manajemen memerlukan izin tambahan yang tidak disediakan dalam kebijakan ini. Untuk melakukan tindakan

ini disarankan untuk menambahkan izin untuk `organizations:PutResourcePolicy` atau melampirkan AWSOrganizationsFullAccess kebijakan.

Detail izin

Kebijakan ini mencakup izin berikut:

- `organizations:ListAccounts`- Memungkinkan kepala sekolah untuk mengambil daftar akun yang merupakan bagian dari organisasi.
- `organizations:DescribeOrganization`- Memungkinkan kepala sekolah untuk mengambil informasi tentang organisasi.
- `organizations:ListRoots`- Memungkinkan kepala sekolah untuk membuat daftar akar organisasi.
- `organizations:ListDelegatedAdministrators`- Memungkinkan kepala sekolah untuk membuat daftar administrator yang didelegasikan dari suatu organisasi.
- `organizations:ListAWSServiceAccessForOrganization`- Memungkinkan kepala sekolah untuk membuat daftar Layanan AWS yang digunakan organisasi.
- `organizations:ListOrganizationalUnitsForParent`- Memungkinkan kepala sekolah untuk membuat daftar unit organisasi anak (OU) dari OU induk.
- `organizations:ListAccountsForParent`- Memungkinkan kepala sekolah untuk mencantumkan akun anak dari OU induk.
- `organizations:ListParents`— Mencantumkan unit akar atau organisasi (OU) yang berfungsi sebagai induk langsung dari OU atau akun anak yang ditentukan.
- `organizations:DescribeAccount` – Memungkinkan principal mengambil informasi tentang akun di organisasi.
- `organizations:DescribeOrganizationalUnit`- Memungkinkan kepala sekolah untuk mengambil informasi tentang OU dalam organisasi.
- `organizations:ListPolicies`— Mengambil daftar semua kebijakan dalam organisasi dari jenis tertentu.
- `organizations:ListPoliciesForTarget`— Mencantumkan kebijakan yang dilampirkan langsung ke root target, unit organisasi (OU), atau akun yang ditentukan.
- `organizations:ListTargetsForPolicy`— Mencantumkan semua akar, unit organisasi (OU), dan akun yang dilampirkan kebijakan tertentu.
- `organizations:EnableAWSServiceAccess`- Memungkinkan kepala sekolah untuk mengaktifkan integrasi dengan Organisasi.

- `organizations:RegisterDelegatedAdministrator`— Memungkinkan kepala sekolah untuk menunjuk akun administrator yang didelegasikan.
- `organizations:DeregisterDelegatedAdministrator`- Memungkinkan kepala sekolah untuk menghapus akun administrator yang didelegasikan.
- `organizations:DescribePolicy`Mengambil informasi tentang kebijakan.
- `organizations:DescribeEffectivePolicy`— Mengembalikan isi kebijakan efektif untuk jenis kebijakan dan akun tertentu.
- `organizations:CreatePolicy`— Membuat kebijakan dari jenis tertentu yang dapat Anda lampirkan ke root, unit organisasi (OU), atau AWS akun individual.
- `organizations:UpdatePolicy`— Memperbarui kebijakan yang ada dengan nama, deskripsi, atau konten baru.
- `organizations:DeletePolicy`— Menghapus kebijakan yang ditentukan dari organisasi Anda.
- `organizations:AttachPolicy`Melampirkan kebijakan ke root, unit organisasi (OU), atau akun individu.
- `organizations:DetachPolicy`Melepaskan kebijakan dari root target, unit organisasi (OU), atau akun.
- `organizations:EnablePolicyType`— Mengaktifkan jenis kebijakan di root.
- `organizations:DisablePolicyType`— Menonaktifkan jenis kebijakan organisasi di root.
- `organizations:TagResource`— Menambahkan satu atau lebih tag ke sumber daya tertentu.
- `organizations:UntagResource`— Menghapus tag apa pun dengan kunci yang ditentukan dari sumber daya tertentu.
- `organizations:ListTagsForResource`— Mencantumkan tag yang dilampirkan ke sumber daya tertentu.
- `organizations:DescribeResourcePolicy`Mengambil informasi tentang kebijakan sumber daya.

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubOrganizationsAccess di Panduan Referensi AWS Kebijakan Terkelola.

AWS kebijakan yang dikelola: AWSSecurityHubServiceRolePolicy

Anda tidak dapat melampirkan `AWSSecurityHubServiceRolePolicy` ke entitas IAM Anda. Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan Security Hub CSPM

melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called "Service-linked peran".

Kebijakan ini memberikan izin administratif yang memungkinkan peran terkait layanan untuk melakukan tugas seperti menjalankan pemeriksaan keamanan untuk kontrol CSPM Security Hub.

Detail izin

Kebijakan ini mencakup izin berikut:

- `cloudtrail`— Ambil informasi tentang jalan set CloudTrail apak.
- `cloudwatch`— Ambil CloudWatch alarm saat ini dan metrik kesehatan Konektor.
- `logs`— Ambil filter metrik untuk CloudWatch log.
- `sns`— Ambil daftar langganan ke topik SNS.
- `config`— Ambil informasi tentang perekam konfigurasi, sumber daya, dan AWS Config aturan. Kelola perekam konfigurasi terkait layanan Security Hub CSPM dan perekam konfigurasi terkait layanan pihak ketiga. Buat dan hapus AWS Config aturan, dan jalankan evaluasi terhadap aturan. Buat daftar perekam konfigurasi dan dapatkan informasi konektor untuk mendukung integrasi cloud pihak ketiga.
- `iam`— Ambil dan buat laporan kredensi untuk akun, dan buat peran terkait layanan untuk. AWS Config
- `organizations`Mengambil informasi akun dan unit organisasi (OU) untuk suatu organisasi.
- `securityhub`— Ambil informasi tentang bagaimana layanan, standar, dan kontrol Security Hub CSPM dikonfigurasi.
- `tag`— Mengambil informasi tentang tag sumber daya.

Untuk meninjau izin kebijakan ini, lihat AWSSecurityHubServiceRolePolicy di Panduan Referensi AWS Kebijakan Terkelola.

Pembaruan Hub Keamanan ke AWS kebijakan terkelola

Tabel berikut memberikan rincian tentang pembaruan kebijakan ter AWS kelola untuk AWS Security Hub dan Security Hub CSPM sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang pembaruan kebijakan, berlangganan umpan RSS di halaman riwayat dokumen Hub Keamanan.

Ubah	Deskripsi	Date
AWSSecurityHubServiceRolePolicy— Kebijakan yang diperbarui	Security Hub CSPM memperbarui kebijakan untuk mendukung integrasi pihak ketiga. Pembaruan menambahkan izin berikut: mengelola perekam konfigurasi pihak ketiga, daftar perekam konfigurasi, dapatkan informasi konektor, dan ambil metrik kesehatan Konektor.	Juni 30, 2026
AWSSecurityHubServiceRolePolicy— Kebijakan yang diperbarui	Security Hub CSPM memperbarui kebijakan untuk menambahkan izin untuk mengelola perekam konfigurasi terkait layanan Security Hub CSPM dan membuat peran terkait layanan. AWS Config	April 29, 2026
AWSSecurityHubOrganizationsAccess— Kebijakan yang diperbarui	Security Hub memperbarui kebijakan untuk menambahkan izin untuk menjelaskan kebijakan sumber daya untuk mendukung fitur Hub Keamanan. Security Hub dalam rilis pratinjau dan dapat berubah.	12 November 2025
AWSSecurityHubFullAccess— Kebijakan yang diperbarui	Security Hub memperbarui kebijakan untuk menambahkan kemampuan seputar pengelolaan GuardDuty , Amazon Inspector, dan manajemen akun untuk mendukung fitur Hub	November 17, 2025

Ubah	Deskripsi	Date
	Keamanan. Security Hub dalam rilis pratinjau dan dapat berubah.	
AWSSecurityHubOrganizationsAccess – Pembaruan ke kebijakan yang ada	Security Hub menambahkan izin baru ke kebijakan. Izin memungkinkan manajemen organisasi untuk mengaktifkan dan mengelola Security Hub dan Security Hub CSPM untuk organisasi.	Juni 17, 2025
AWSSecurityHubFullAccess – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan izin baru yang memungkinkan prinsipal membuat peran terkait layanan untuk Hub Keamanan.	Juni 17, 2025
AWSSecurityHubFullAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan untuk mendapatkan detail harga untuk Layanan AWS dan produk.	April 24, 2024
AWSSecurityHubReadOnlyAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan terkelola ini dengan menambahkan bidang. `Sid`	Februari 22, 2024

Ubah	Deskripsi	Date
AWSSecurityHubFullAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan sehingga dapat menentukan apakah Amazon GuardDuty dan Amazon Inspector diaktifkan di akun. Ini membantu pelanggan menyatukan informasi terkait keamanan dari banyak orang. Layanan AWS	16 November 2023
AWSSecurityHubOrganizationsAccess— Perbarui ke kebijakan yang ada	Security Hub CSPM memperbarui kebijakan untuk memberikan izin tambahan untuk mengizinkan akses baca-saja ke fungsionalitas administrator yang didelegasikan AWS Organizations . Ini termasuk detail seperti root, unit organisasi (OU), akun, struktur organisasi, dan akses layanan.	16 November 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan `BatchGetSecurityControls` , `DisassociateFromAdministratorAccount` , dan `UpdateSecurityControl` izin untuk membaca dan memperbarui properti kontrol keamanan yang dapat disesuaikan.	26 November 2023

Ubah	Deskripsi	Date
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan `tag:GetResources` izin untuk membaca tag sumber daya yang terkait dengan temuan.	7 November 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan `BatchGetStandardsControlAssociations` izin untuk mendapatkan informasi tentang status pengaktifan kontrol dalam standar.	27 September 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan izin baru untuk mendapatkan AWS Organizations data dan membaca serta memperbarui konfigurasi CSPM Security Hub, termasuk standar dan kontrol.	20 September 2023
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM memindahkan `config:DescribeConfigRuleEvaluationStatus` izin yang ada ke pernyataan yang berbeda dalam kebijakan. Iz `config:DescribeConfigRuleEvaluationStatus` in sekarang diterapkan ke semua sumber daya.	Maret 17, 2023

Ubah	Deskripsi	Date
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM memindahkan `config:PutEvaluations` izin yang ada ke pernyataan yang berbeda dalam kebijakan. Iz `config:PutEvaluations` in sekarang diterapkan ke semua sumber daya.	14 Juli 2021
AWSSecurityHubServiceRolePolicy – Pembaruan ke kebijakan yang ada	Security Hub CSPM menambahkan izin baru untuk memungkinkan peran terkait layanan untuk memberikan hasil evaluasi ke. AWS Config	29 Juni 2021
AWSSecurityHubServiceRolePolicy— Ditambahkan ke daftar kebijakan yang dikelola	Menambahkan informasi tentang kebijakan terkelola AWSSecurityHubServiceRolePolicy, yang digunakan oleh peran terkait layanan CSPM Hub Keamanan.	11 Juni 2021
AWSSecurityHubOrganizationsAccess— Kebijakan baru	Security Hub CSPM menambahkan kebijakan baru yang memberikan izin yang diperlukan untuk integrasi Security Hub CSPM dengan Organisasi.	15 Maret 2021
Security Hub CSPM mulai melacak perubahan	Security Hub CSPM mulai melacak perubahan untuk kebijakan yang AWS dikelolanya.	15 Maret 2021

Pemecahan masalah AWS Security Hub CSPM Identitas dan Akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Security Hub CSPM dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Security Hub CSPM
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin akses terprogram ke Security Hub CSPM
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses Security Hub CSPM
- Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya CSPM Security Hub saya

Saya tidak berwenang untuk melakukan tindakan di Security Hub CSPM

Jika member Konsol Manajemen AWS itahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang *`widget`* tetapi tidak memiliki `securityhub:`*`GetWidget`* izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya *`my-example-widget`* menggunakan tindakan `securityhub:`*`GetWidget`*.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan tersebut, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Hub Keamanan.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan itu alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Hub Keamanan. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya ingin akses terprogram ke Security Hub CSPM

Pengguna memerlukan akses terprogram jika mereka ingin berinteraksi dengan AWS di luar. Konsol Manajemen AWS Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Disarankan) Gunakan kredenSIAL konsol sebagai kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Login untuk pengembangan AWS lokal di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, lihat Login untuk pengembangan AWS lokal di Panduan

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		Refer AWS ensi SDK dan Alat.
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Meng onfigurasi AWS CLI untuk digunakan AWS IAM Identity Center di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat otentikasi Pusat Identitas IAM di Panduan Refer AWS ensi SDK dan Alat.
IAM	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk dalam Menggunakan kredenSIAL sementara dengan AWS sumber daya di Panduan Pengguna IAM.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Tidak direkomendasikan) Gunakan kredentif jangka panjang untuk menandata ngani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk itu AWS CLI, lihat Meng autentikasi menggunakan kredentif pengguna IAM di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK dan alat, lihat Meng autentikasi menggunakan kredentif jangka panjang di Panduan Refer AWS ensi SDK dan Alat. • Untuk AWS API, lihat M engelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Security Hub CSPM

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Saya ingin mengizinkan orang-orang di luar saya Akun AWS untuk mengakses sumber daya CSPM Security Hub saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Security Hub mendukung fitur-fitur ini, lihatCara kerja Security Hub dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM lainnya Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyedi Akun AWS akan akses milik pihak ketiga di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk AWS Security Hub CSPM

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi ingin menggunakannya AWS untuk beban kerja yang diatur, Anda dapat mendaftar untuk AWS (lanjutan) atau mengaktifkan fitur lanjutan untuk lingkungan Anda AWS .

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup berdasarkan Program Kepatuhan dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program Kep AWS atuhan Program Jaminan .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi AWS Keamanan.

Ketahanan di AWS Hub Keamanan

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Zona Ketersediaan. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Zona Ketersediaan, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di AWS Security Hub CSPM

Sebagai layanan terkelola, AWS Security Hub CSPM dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat AWS Keamanan Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infra struktur di Security Pillar AWS Well-Architected Framework.

Anda menggunakan panggilan API yang di AWS publikasikan untuk mengakses Security Hub CSPM melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Suite Cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

AWS Security Hub CSPM dan antarmuka titik akhir VPC (AWS PrivateLink)

Anda dapat membuat koneksi pribadi antara VPC Anda dan AWS Security Hub CSPM dengan membuat titik akhir VPC antarmuka. Titik akhir antarmuka didukung oleh AWS PrivateLink, teknologi yang memungkinkan Anda mengakses API CSPM Security Hub secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi AWS Direct Connect. Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Security Hub CSPM API. Lalu lintas antara VPC dan Security Hub CSPM Anda tidak meninggalkan jaringan Amazon.

Setiap titik akhir antarmuka diwakili oleh satu atau beberapa Antarmuka Jaringan Elastis di subnet Anda. Untuk informasi selengkapnya, lihat Meng akses titik akhir VPC Layanan AWS menggunakan antarmuka di Panduan Amazon Virtual Private Cloud.

Pertimbangan untuk titik akhir VPC Security Hub CSPM

Sebelum menyiapkan titik akhir VPC antarmuka untuk Security Hub CSPM, pastikan Anda meninjau prasyarat dan informasi lainnya di Panduan Amazon Virtual Private Cloud.

Security Hub CSPM mendukung panggilan ke semua tindakan API-nya dari VPC Anda.

Membuat titik akhir antarmuka VPC untuk Security Hub CSPM

Anda dapat membuat titik akhir VPC untuk layanan CSPM Security Hub menggunakan konsol Amazon VPC atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir VPC di Panduan Amazon Virtual Private Cloud.

Buat titik akhir VPC untuk Security Hub CSPM menggunakan nama layanan berikut:

`com.amazonaws.`*`region`*`.securityhub`

Di *`region`* mana kode Wilayah untuk yang berlaku Wilayah AWS.

Jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Security Hub CSPM menggunakan nama DNS default untuk Wilayah, misalnya, `securityhub.us-east-1.amazonaws.com` untuk Wilayah AS Timur (Virginia Utara).

Membuat kebijakan titik akhir VPC untuk Security Hub CSPM

Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC yang mengontrol akses ke Security Hub CSPM. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir di Panduan Amazon Virtual Private Cloud.

Contoh: Kebijakan titik akhir VPC untuk tindakan CSPM Hub Keamanan

Berikut ini adalah contoh kebijakan titik akhir untuk Security Hub CSPM. Saat dilampirkan ke titik akhir, kebijakan ini memberikan akses ke tindakan CSPM Hub Keamanan yang terdaftar untuk semua prinsipal di semua sumber daya.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

Subnet bersama

Anda tidak dapat membuat, mendeskripsikan, memodifikasi, atau menghapus titik akhir VPC di subnet yang dibagikan dengan Anda. Namun, Anda dapat menggunakan titik akhir VPC di subnet yang dibagikan dengan Anda. Untuk informasi tentang berbagi VPC, lihat Mem bagikan subnet VPC Anda dengan akun lain di Panduan Amazon Virtual Private Cloud.

Mencatat panggilan API Security Hub dengan CloudTrail

AWSSecurity Hub CSPM terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Security Hub CSPM. CloudTrail

menangkap panggilan API untuk Security Hub CSPM sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan dari konsol CSPM Security Hub dan panggilan kode ke operasi API CSPM Security Hub. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Security Hub CSPM. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang CloudTrail dikumpulkan, Anda dapat menentukan permintaan yang dibuat ke Security Hub CSPM, alamat IP tempat permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

Informasi CSPM Security Hub di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas peristiwa yang didukung terjadi di Security Hub CSPM, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun . Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan peristiwa yang sedang berlangsung di akun Anda, termasuk acara untuk Security Hub CSPM, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, ketika Anda membuat jejak pada konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa wilayah dan Menerima file CloudTrail log dari beberapa akun

Security Hub CSPM mendukung pencatatan semua tindakan Security Hub CSPM API sebagai peristiwa dalam log. CloudTrail Untuk melihat daftar operasi CSPM Security Hub, lihat Referensi API CSPM Security Hub.

Saat aktivitas untuk tindakan berikut dicatat CloudTrail, nilai untuk `responseElements` disetel ke`null`. Ini memastikan bahwa informasi sensitif tidak disertakan dalam CloudTrail log.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan root atau AWS Identity and Access Management (IAM) kredensional pengguna
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan
- Apakah permintaan itu dibuat oleh AWS layanan lain

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Contoh: Entri file log CSPM Security Hub

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `CreateInsight` tindakan. Dalam contoh ini, sebuah wawasan yang `Test Insight` disebut dibuat. `ResourceId`Atribut ditetapkan sebagai Grup menurut agregator, dan tidak ada filter opsional untuk wawasan ini yang ditentukan. Untuk informasi selengkapnya tentang wawasan, lihat Melihat wawasan di Security Hub CSPM.

```
{
```

```
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJK6U5DS22IAVUI7BW",
        "arn": "arn:aws:iam::012345678901:user/TestUser",
        "accountId": "012345678901",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "TestUser"
    },
    "eventTime": "2018-11-25T01:02:18Z",
    "eventSource": "securityhub.amazonaws.com",
    "eventName": "CreateInsight",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
    "requestParameters": {
        "Filters": {},
        "ResultField": "ResourceId",
        "Name": "Test Insight"
    },
    "responseElements": {
        "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/
f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
    },
    "requestID": "c0fffccd-f04d-11e8-93fc-ddcd14710066",
    "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "012345678901"
}
```

Menandai sumber daya Security Hub

Tag adalah label opsional yang dapat Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya CSPM AWS Security Hub tertentu. Tag dapat membantu Anda mengidentifikasi, mengategorikan, dan mengelola sumber daya dengan cara yang berbeda-beda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk membedakan sumber daya, mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu, atau mengalokasikan biaya.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Menandai dasar-dasar

Sumber daya dapat memiliki sebanyak 50 tag. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional, yang keduanya Anda tentukan. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Misalnya, jika Anda membuat aturan otomatisasi yang berbeda untuk lingkungan yang berbeda (satu set aturan otomatisasi untuk akun pengujian dan satu lagi untuk akun produksi), Anda dapat menetapkan kunci `Environment` tag untuk aturan tersebut. Nilai tag terkait mungkin `Test` untuk aturan yang terkait dengan akun pengujian, dan `Prod` untuk aturan yang terkait dengan akun produksi dan OU.

Saat Anda menentukan dan menetapkan tag ke sumber daya CSPM AWS Security Hub, ingatlah hal berikut:

- Setiap sumber daya dapat memiliki maksimum 50 tag.
- Untuk setiap sumber daya, setiap kunci tag harus unik dan hanya dapat memiliki satu nilai tag.
- Kunci dan nilai tag peka huruf besar/kecil. Sebagai praktik terbaik, kami menyarankan Anda menentukan strategi untuk memanfaatkan tag dan menerapkan strategi itu secara konsisten di seluruh sumber daya Anda.

- Tombol tag dapat memiliki maksimal 128 UTF-8 karakter. Nilai tag dapat memiliki maksimal 256 UTF-8 karakter. Karakter dapat berupa huruf, angka, spasi, atau simbol berikut: _.:/= + - @
- `aws:`Awalan dicadangkan untuk digunakan olehAWS. Anda tidak dapat menggunakannya dalam kunci tag atau nilai apa pun yang Anda tentukan. Selain itu, Anda tidak dapat mengubah atau menghapus kunci tag atau nilai yang menggunakan awalan ini. Tag yang menggunakan awalan ini tidak dihitung terhadap kuota 50 tag per sumber daya.
- Setiap tag yang Anda tetapkan hanya tersedia untuk Anda Akun AWS dan hanya Wilayah AWS di mana Anda menetapkannya.
- Jika Anda menetapkan tag ke sumber daya menggunakan CSPM Security Hub, tag hanya diterapkan ke sumber daya yang disimpan langsung di CSPM Security Hub di yang berlaku. Wilayah AWS Mereka tidak diterapkan pada sumber daya pendukung terkait yang dibuat, digunakan, atau dikelola oleh Security Hub CSPM untuk Anda di tempat lain. Layanan AWS Misalnya, jika Anda menetapkan tag ke aturan otomatisasi yang memperbarui temuan yang terkait dengan Amazon Simple Storage Service (Amazon S3), tag hanya diterapkan ke aturan otomatisasi di CSPM Security Hub untuk Wilayah yang ditentukan. Mereka tidak diterapkan ke ember S3 Anda. Untuk juga menetapkan tag ke sumber daya terkait, Anda dapat menggunakan AWS Resource Groups atau Layanan AWS yang menyimpan sumber daya—misalnya, Amazon S3 untuk bucket S3. Menetapkan tag ke sumber daya terkait dapat membantu Anda mengidentifikasi sumber daya pendukung untuk sumber daya CSPM Security Hub Anda.
- Jika Anda menghapus sumber daya, tag apa pun yang ditetapkan ke sumber daya juga akan dihapus.

> **Important**
>
> Jangan menyimpan rahasia atau jenis data sensitif lainnya dalam tag. Tag dapat diakses dari banyak orangLayanan AWS, termasukAWS Manajemen Penagihan dan Biaya. Mereka tidak dimaksudkan untuk digunakan untuk data sensitif.

Untuk menambahkan dan mengelola tag untuk sumber daya CSPM Security Hub, Anda dapat menggunakan konsol CSPM Security Hub, Security Hub CSPM API, atau API Tagging. AWS Resource Groups Dengan Security Hub CSPM, Anda dapat menambahkan tag ke sumber daya saat membuat sumber daya. Anda juga dapat menambahkan dan mengelola tag untuk sumber daya individual yang ada. Dengan Resource Groups, Anda dapat menambahkan dan mengelola tag

secara massal untuk beberapa sumber daya yang ada mencakup beberapaLayanan AWS, termasuk Security Hub CSPM.

Untuk tips penandaan tambahan dan praktik terbaik, lihat Menandai AWS sumber daya Anda di Panduan Pengguna Tagging AWS Resources.

Menggunakan tag dalam kebijakan IAM

Setelah mulai menandai sumber daya, Anda dapat menentukan izin tingkat sumber daya berbasis tag dalam kebijakan (IAM). AWS Identity and Access Management Dengan menggunakan tag dengan cara ini, Anda dapat menerapkan kontrol terperinci tentang pengguna dan peran mana yang Akun AWS memiliki izin untuk membuat dan menandai sumber daya, dan pengguna dan peran mana yang memiliki izin untuk menambahkan, mengedit, dan menghapus tag secara lebih umum. Untuk mengontrol akses berdasarkan tag, Anda dapat menggunakan kunci kondisi terkait tag di elemen Kondisi kebijakan IAM.

Misalnya, Anda dapat membuat kebijakan IAM yang memungkinkan pengguna memiliki akses penuh ke semua sumber daya CSPM AWS Security Hub, jika `Owner` tag untuk sumber daya menentukan nama pengguna mereka:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

Jika Anda menentukan izin tingkat sumber daya berbasis tag, izin akan segera berlaku. Ini berarti bahwa sumber daya Anda lebih aman segera setelah dibuat, dan Anda dapat dengan cepat mulai menerapkan penggunaan tag untuk sumber daya baru. Anda juga dapat menggunakan izin tingkat sumber daya untuk mengontrol kunci dan nilai tag mana yang dapat dikaitkan dengan sumber daya baru dan yang sudah ada. Untuk informasi selengkapnya, lihat Mengontrol akses ke AWS sumber daya menggunakan tag di Panduan Pengguna IAM.

Menambahkan tag ke sumber daya CSPM Security Hub

Tag adalah label yang dapat Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya CSPM AWS Security Hub tertentu. Dengan menggunakan tag, Anda dapat mengidentifikasi, mengkategorikan, dan mengelola sumber daya dengan cara yang berbeda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk: menerapkan kebijakan, mengalokasikan biaya, membedakan antara versi sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Sumber daya dapat memiliki sebanyak 50 tag. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag. Untuk informasi selengkapnya tentang opsi dan persyaratan penandaan, lihatMenandai dasar-dasar.

Untuk menambahkan tag ke sumber daya CSPM Security Hub, Anda dapat menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Namun, konsol tidak mendukung penambahan tag ke Hub sumber daya.

Setelah menambahkan tag, Anda dapat mengedit tag dan mengubah kunci tag atau nilai tag.

Untuk menambahkan atau mengedit tag untuk beberapa sumber daya CSPM Security Hub secara bersamaan, gunakan operasi penandaan API Penandaan. AWS Resource Groups

> **Important**
>
> Menambahkan tag ke sumber daya dapat memengaruhi akses ke sumber daya. Sebelum menambahkan tag ke sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Console

Untuk menambahkan tag ke sumber daya CSPM Security Hub (konsol)

Saat Anda membuat aturan otomatisasi atau kebijakan konfigurasi, konsol CSPM Security Hub menyediakan opsi untuk menambahkan tag ke dalamnya. Anda dapat memberikan kunci tag dan nilai tag di bagian Tag.

Security Hub CSPM API

Untuk menambahkan tag ke sumber daya CSPM Security Hub (API)

Untuk membuat sumber daya dan menambahkan satu atau beberapa tag ke dalamnya secara terprogram, gunakan operasi yang sesuai untuk jenis sumber daya yang ingin Anda buat:

- Untuk membuat kebijakan konfigurasi dan menambahkan satu atau beberapa tag ke dalamnya, panggil CreateConfigurationPolicyAPI atau, jika Anda menggunakanAWS CLI, jalankan perintah create-configuration-policy.
- Untuk membuat aturan otomatisasi dan menambahkan satu atau beberapa tag ke dalamnya, panggil CreateAutomationRuleAPI atau, jika Anda menggunakanAWS CLI, jalankan perintah create-automation-rule.
- Untuk mengaktifkan CSPM Security Hub dan menambahkan satu atau beberapa tag ke Hub sumber daya Anda, jalankan EnableSecurityHubAPI atau, jika Anda menggunakan AWS Command Line Interface (AWS CLI), jalankan perintah enable-security-hub.

Dalam permintaan Anda, gunakan `tags` parameter untuk menentukan kunci tag dan nilai tag opsional untuk setiap tag untuk ditambahkan ke sumber daya. `tags`Parameter menentukan array objek. Setiap objek menentukan kunci tag dan nilai tag yang terkait.

Untuk menambahkan satu atau beberapa tag ke sumber daya yang ada, gunakan TagResourcepengoperasian API CSPM Security Hub atau, jika Anda menggunakanAWS

CLI, jalankan perintah tag-resource. Dalam permintaan Anda, tentukan Nama Sumber Daya Amazon (ARN) dari sumber daya yang ingin Anda tambahkan tag. Gunakan `tags` parameter untuk menentukan kunci tag (`key`) dan nilai tag opsional (`value`) untuk setiap tag yang akan ditambahkan. `tags`Parameter menentukan array objek, satu objek untuk setiap kunci tag dan nilai tag terkait.

Misalnya, AWS CLI perintah berikut menambahkan kunci `Environment` tag dengan nilai `Prod` tag ke kebijakan konfigurasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

Contoh perintah CLI:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

Di mana:

- `resource-arn`menentukan ARN dari kebijakan konfigurasi untuk menambahkan tag ke.
- *`Environment`*adalah kunci tag tag untuk ditambahkan ke aturan.
- *`Prod`*adalah nilai tag untuk kunci tag tertentu (*`Environment`*).

Dalam contoh berikut, perintah menambahkan beberapa tag ke kebijakan konfigurasi.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod", "CostCenter":"12345", "Owner":"jane-doe"}'
```

Untuk setiap objek dalam `tags` array, keduanya `key` dan `value` argumen diperlukan. Namun, nilai untuk `value` argumen dapat berupa string kosong. Jika Anda tidak ingin mengaitkan nilai tag dengan kunci tag, jangan tentukan nilai untuk `value` argumen tersebut. Misalnya, perintah berikut menambahkan kunci `Owner` tag tanpa nilai tag terkait:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
```

```
--tags '{"Owner":""}'
```

Jika operasi penandaan berhasil, Security Hub CSPM mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub CSPM mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Mengedit tag untuk sumber daya CSPM Security Hub

Karena lingkungan atau persyaratan Anda berubah seiring waktu, Anda dapat mengevaluasi tag yang ada untuk sumber daya CSPM AWS Security Hub dan mengubah tag seperlunya. Tag adalah label yang Anda tentukan dan tetapkan ke satu atau beberapa AWS sumber daya, termasuk jenis sumber daya Macie tertentu. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Tag dapat membantu Anda mengidentifikasi, mengategorikan, dan mengelola sumber daya dengan cara yang berbeda-beda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk: menerapkan kebijakan, mengalokasikan biaya, membedakan antara versi sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Untuk mengedit kunci tag atau nilai tag untuk sumber daya CSPM Security Hub, Anda dapat menggunakan Security Hub CSPM API. Konsol CSPM Security Hub saat ini tidak mendukung pengeditan tag.

> **Important**
>
> Mengedit tag untuk sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda mengedit tag untuk sumber daya, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Security Hub CSPM API

Untuk mengedit tag untuk sumber daya CSPM Security Hub (API)

Saat Anda mengedit tag untuk sumber daya secara terprogram, Anda menimpa tag yang ada dengan nilai baru. Oleh karena itu, cara terbaik untuk mengedit tag tergantung pada apakah Anda ingin mengedit kunci tag, nilai tag, atau keduanya. Untuk mengedit kunci tag, hapus tag saat ini dan tambahkan tag baru.

Untuk mengedit atau menghapus hanya nilai tag yang terkait dengan kunci tag, timpa nilai yang ada dengan menggunakan TagResourcepengoperasian Security Hub CSPM API. Jika Anda menggunakanAWS CLI, jalankan perintah tag-resource. Dalam permintaan Anda, tentukan Nama Sumber Daya Amazon (ARN) sumber daya yang nilai tagnya ingin Anda edit atau hapus.

Untuk mengedit nilai tag, gunakan `tags` parameter untuk menentukan kunci tag yang nilai tag yang ingin Anda ubah. Anda juga harus menentukan nilai tag baru untuk kunci tersebut. Misalnya, AWS CLI perintah berikut mengubah nilai tag dari `Prod` menjadi kunci `Test Environment` tag yang ditetapkan ke aturan otomatisasi yang ditentukan. Contoh ini diformat untuk Linux, macOS, atau Unix, dan menggunakan karakter garis miring terbalik (\) untuk meningkatkan keterbacaan.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

Di mana:

- `resource-arn`menentukan ARN dari kebijakan konfigurasi.
- *`Environment`*adalah kunci tag yang terkait dengan nilai tag untuk diubah.
- *`Test`*adalah nilai tag baru untuk kunci tag tertentu (*`Environment`*).

Untuk menghapus nilai tag dari kunci tag, jangan tentukan nilai untuk `value` argumen kunci dalam `tags` parameter. Contoh:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

Jika operasi berhasil, Security Hub CSPM mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub CSPM mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Meninjau tag untuk sumber daya CSPM Security Hub

Setelah menambahkan atau mengedit tag untuk sumber daya CSPM AWS Security Hub, Anda dapat melihat kunci tag dan nilai tag yang dimiliki sumber daya saat ini. Tag adalah label yang Anda tentukan dan tetapkan ke satu atau beberapa AWS sumber daya, termasuk jenis sumber daya Macie tertentu. Setiap tag terdiri dari kunci tag yang diperlukan dan nilai tag opsional. Kunci tag adalah label umum yang bertindak sebagai kategori untuk nilai tag yang lebih spesifik. Nilai tag bertindak sebagai deskriptor untuk kunci tag.

Tag dapat membantu Anda mengidentifikasi, mengategorikan, dan mengelola sumber daya dengan cara yang berbeda-beda, seperti berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Misalnya, Anda dapat menggunakan tag untuk: menerapkan kebijakan, mengalokasikan biaya, membedakan antara versi sumber daya, atau mengidentifikasi sumber daya yang mendukung persyaratan kepatuhan atau alur kerja tertentu.

Anda dapat menambahkan tag ke jenis sumber daya CSPM Security Hub berikut:

- Aturan otomatisasi
- Kebijakan konfigurasi
- Sumber daya Hub

Anda dapat meninjau tag untuk aturan otomatisasi CSPM Security Hub atau kebijakan konfigurasi dengan menggunakan konsol CSPM Security Hub atau Security Hub CSPM API. Konsol tidak mendukung tag peninjauan untuk Hub sumber daya. Secara terprogram, Anda dapat meninjau tag untuk sumber daya apa pun.

Untuk meninjau tag untuk beberapa sumber daya CSPM Security Hub secara bersamaan, gunakan operasi penandaan API Penandaan. AWS Resource Groups

Console

Untuk meninjau tag untuk sumber daya CSPM Security Hub (konsol)

1. Menggunakan kredensi administrator CSPM Security Hub, buka konsol CSPM Security Hub AWS di. https://console.aws.amazon.com/securityhub/
2. Bergantung pada jenis sumber daya yang ingin Anda tambahkan tag, lakukan salah satu hal berikut:
   - Untuk meninjau tag untuk aturan otomatisasi, pilih Otomasi di panel navigasi. Kemudian, pilih aturan otomatisasi.
   - Untuk meninjau tag untuk kebijakan konfigurasi, pilih Konfigurasi di panel navigasi. Kemudian, pada tab Kebijakan, pilih opsi di sebelah kebijakan konfigurasi. Panel samping terbuka yang menunjukkan jumlah tag yang ditetapkan ke kebijakan. Anda dapat memperluas header Tag untuk melihat kunci tag dan nilai tag.

Bagian Tag mencantumkan semua tag yang saat ini ditetapkan ke sumber daya.

Security Hub CSPM API

Untuk meninjau tag untuk sumber daya CSPM Security Hub (API)

Untuk mengambil dan meninjau tag untuk sumber daya yang ada, panggil API. ListTagsForResource Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) sumber daya.

Jika Anda menggunakanAWS CLI, jalankan perintah list-tags-for-resource dan gunakan parameter `resource-arn` untuk menentukan ARN sumber daya. Contoh:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Jika operasi berhasil, Security Hub CSPM mengembalikan array. `tags` Setiap objek dalam array menentukan tag (baik kunci tag dan nilai tag) yang saat ini ditetapkan ke sumber daya. Contoh:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
```

```
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
}
```

Di mana `EnvironmentCostCenter`,, dan `Owner` merupakan kunci tag yang ditetapkan ke sumber daya. `Prod`adalah nilai tag yang terkait dengan kunci `Environment` tag. `12345`adalah nilai tag yang terkait dengan kunci `CostCenter` tag. Kunci `Owner` tag tidak memiliki nilai tag terkait.

Untuk mengambil daftar semua sumber daya CSPM Security Hub yang memiliki tag dan semua tag yang ditetapkan ke masing-masing sumber daya tersebut, gunakan GetResourcespengoperasian API Tagging. AWS Resource Groups Dalam permintaan Anda, tetapkan nilai untuk `ResourceTypeFilters` parameter ke`securityhub`. Untuk melakukan ini menggunakanAWS CLI, jalankan perintah get-resources dan atur nilai untuk `resource-type-filters` parameter ke. `securityhub` Contoh:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

Jika operasi berhasil, Resource Groups mengembalikan `ResourceTagMappingList` array. Array berisi satu objek untuk setiap sumber daya CSPM Security Hub yang memiliki tag. Setiap objek menentukan ARN sumber daya CSPM Security Hub, dan kunci tag serta nilai yang ditetapkan ke sumber daya.

Menghapus tag dari sumber daya CSPM Security Hub

Jika Anda menambahkan tag ke sumber daya CSPM AWS Security Hub, Anda selanjutnya dapat menghapus satu atau beberapa tag. Tag adalah label yang Anda tentukan dan tetapkan ke AWS sumber daya, termasuk jenis sumber daya CSPM Security Hub tertentu. Anda dapat menambahkan, mengedit, dan menghapus tag dari jenis sumber daya CSPM Security Hub berikut: aturan otomatisasi, kebijakan konfigurasi, dan sumber daya. Hub

Untuk menghapus tag dari sumber daya CSPM AWS Security Hub individual, Anda dapat menggunakan Security Hub CSPM API. Konsol CSPM Security Hub saat ini tidak mendukung penghapusan tag.

Untuk menghapus tag dari beberapa sumber daya CSPM Security Hub secara bersamaan, gunakan operasi penandaan API Penandaan. AWS Resource Groups

> **Important**
>
> Menghapus tag dari sumber daya dapat memengaruhi akses ke sumber daya. Sebelum Anda menghapus tag, tinjau kebijakan AWS Identity and Access Management (IAM) apa pun yang mungkin menggunakan tag untuk mengontrol akses ke sumber daya.

Security Hub CSPM API

Untuk menghapus tag dari sumber daya CSPM Security Hub (API)

Untuk menghapus satu atau beberapa tag dari sumber daya secara terprogram, gunakan UntagResourcepengoperasian Security Hub CSPM API. Dalam permintaan Anda, gunakan `resourceArn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) sumber daya untuk menghapus tag. Gunakan `tagKeys` parameter untuk menentukan kunci tag tag yang akan dihapus. Untuk menghapus beberapa tag, tambahkan `tagKeys` parameter dan argumen untuk setiap tag yang akan dihapus, dipisahkan oleh ampersand (&) —misalnya,. `tagKeys=key1&tagKeys=key2` Untuk menghapus hanya nilai tag tertentu (bukan kunci tag) dari sumber daya, edit tag alih-alih menghapus tag.

Jika Anda menggunakanAWS CLI, jalankan perintah untag-resource untuk menghapus satu atau beberapa tag dari sumber daya. Untuk `resource-arn` parameter, tentukan ARN sumber daya untuk menghapus tag dari. Gunakan `tag-keys` parameter untuk menentukan kunci tag tag yang akan dihapus. Misalnya, perintah berikut menghapus `Environment` tag (kunci tag dan nilai tag) dari kebijakan konfigurasi yang ditentukan:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

Di mana `resource-arn` menentukan ARN dari kebijakan konfigurasi untuk menghapus tag dari, *`Environment`* dan merupakan kunci tag tag untuk dihapus.

Untuk menghapus beberapa tag dari sumber daya, tambahkan setiap kunci tag tambahan sebagai argumen untuk `tag-keys` parameter. Contoh:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

Jika operasi berhasil, Security Hub CSPM mengembalikan respons HTTP 200 kosong. Jika tidak, Security Hub CSPM mengembalikan respons HTTP 4 xx atau 500 yang menunjukkan mengapa operasi gagal.

Kuota untuk Security Hub

Anda Akun AWS memiliki kuota default tertentu, sebelumnya disebut sebagai batas, untuk masing-masing. Layanan AWS Kuota ini merupakan jumlah maksimum layanan sumber daya atau operasi untuk akun Anda. Topik ini menautkan ke kuota yang berlaku untuk sumber daya dan operasi AWS Security Hub untuk akun Anda. Kecuali sebaliknya dinyatakan lain, setiap kuota berlaku untuk akun Anda di setiap Wilayah AWS.

Beberapa kuota dapat ditingkatkan, sementara yang lain tidak bisa. Untuk meminta peningkatan kuota, gunakan konsol Service Quotas. Untuk mempelajari selengkapnya cara menyampaikan permintaan kenaikan kuota, lihat Meminta kenaikan kuota dalam Panduan Pengguna Service Quotas. Jika kuota tidak tersedia di konsol Service Quotas, gunakan formulir peningkatan batas layanan untuk meminta kenaikan kuota. AWS Support Center Console

Kuota maksimum

Untuk daftar kuota yang berlaku untuk sumber daya AWS Security Hub, lihat titik akhir dan kuota AWS Security Hub di. Referensi Umum AWS

Nilai kuota

Untuk daftar kuota yang berlaku untuk operasi API AWS Security Hub, lihat Referensi API AWS Security Hub.

Jika Anda menyiapkan agregasi Lintas wilayah di CSPM Security Hub, satu panggilan ke `BatchImportFindings` dan `BatchUpdateFindings` berdampak pada Wilayah yang ditautkan dan Wilayah agregasi. `GetFindings`Operasi mengambil temuan dari Wilayah terkait dan Wilayah agregasi. Namun, `BatchEnableStandards` dan `UpdateStandardsControl` operasi adalah Region-specific.

Riwayat dokumen untuk AWS Security Hub Panduan Pengguna

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir dari AWS Security Hub dan Security Hub CSPM. Untuk rilis kontrol CSPM Security Hub baru, tanggal menentukan kapan kontrol mulai tersedia di yang didukung. Wilayah AWS Diperlukan waktu 1-2 minggu agar kontrol tersedia di semua Wilayah yang didukung. Untuk detail tentang perubahan material pada kontrol yang ada, lihatLog perubahan untuk kontrol CSPM Security Hub.

Untuk menerima pemberitahuan tentang pembaruan Panduan AWS Pengguna Hub Keamanan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Detail temuan informasi Pemindaian Jaringan yang diperbarui	Menambahkan informasi tentang temuan informasi yang dihasilkan Pemindaian Jaringan.	3 September 2026
Daftar port Pemindaian Jaringan yang Diperbarui	Menambahkan daftar port yang saat ini didukung oleh Pemindaian Jaringan.	Agustus 18, 2026
Kontrol keamanan yang diperbarui	Security Hub CSPM menghapus EFS.6 kontrol dari standar F AWS oundation al Security Best Practices (FSBP). Kontrol ini tetap tersedia dalam standar NIST SP 800-53 Rev. 5, NIST SP 800-171 Revisi 2, dan PCI DSS v4.0.1.	Agustus 3, 2026
Dokumentasi Security Hub yang ditingkatkan	Memperbaiki panduan dalam Mengelola konfigurasi akun	Juli 7, 2026

	anggota di halaman AWS Organisasi.	
Ditambahkan dokumentasi fitur Pemindaian Jaringan	Menambahkan dokumentasi untuk fitur pemindaian Jaringan dari Hub Keamanan	Juli 7, 2026
Inventaris AI	Menambahkan inventaris AI, yang menyediakan tampilan terpadu sumber daya kecerdasan buatan (AI) dan pembelajaran mesin (ML) yang dikelola dan di-host sendiri di seluruh AWS lingkungan Anda. Untuk informasi selengkapnya, lihat inventaris AI di Hub AWS Keamanan.	Juli 7, 2026
Pembaruan untuk kebijakan terkelola - `AWSSecurityHubV2ServiceRolePolicy`	Security Hub memperbarui kebijakan ter AWS kelola bernama`AWSSecurityHubV2ServiceRolePolicy` . Pembaruan menambahkan izin untuk mendukung integrasi pihak ketiga, termasuk mengelola perekam konfigurasi pihak ketiga, membuat dan mengelola konektor, dan memperoleh token identitas web untuk federasi.	Juni 30, 2026

Pembaruan untuk kebijakan terkelola - `AWSSecurityHubServiceRolePolicy`	Security Hub CSPM memperbarui kebijakan terkel AWS ola bernama. `AWSSecurityHubServiceRolePolicy` Pembaruan menambahkan izin untuk mendukung integrasi pihak ketiga. Ini termasuk mengelola perekam konfigurasi pihak ketiga dan mengambil metrik kesehatan Konektor.	Juni 30, 2026
Standar keamanan baru	Security Hub CSPM merilis standar Praktik Terbaik Keamanan AI. Standar ini menyediakan serangkaian kontrol yang dikuratori yang mendeteksi kapan sumber daya AI yang digunakan tidak selaras dengan praktik terbaik keamanan.	Juni 30, 2026
Kontrol keamanan baru	Security Hub CSPM merilis delapan kontrol baru untuk standar Praktik Terbaik Keamanan AI. Kontrol baru adalah: Bedrock.1, BedrockAgentCore.7, SageMaker.20, SageMaker.21, SageMaker.22 SageMaker.23, SageMaker.24, dan SageMaker.25.	Juni 30, 2026

Jenis sifat dampak dan pembaruan tingkat keparahan untuk temuan paparan	Menambahkan jenis sifat Dampak ke temuan paparan. Dampak menggambarkan radius ledakan potensial jika sumber daya dikomprom ikan, berdasarkan izin efektif dari prinsipal AWS Identity and Access Management terkait. Memperbarui perhitung an tingkat keparahan untuk menggunakan matriks risiko Kemungkinan dan Dampak yang selaras dengan panduan NIST. Menambahkan panduan remediasi per sumber daya untuk sifat jalur akses dampak.	Juni 23, 2026
Pembaruan standar dan kontrol keamanan	Kami menghentikan RDS.18 kontrol ECS.1 dan dan menghapusnya dari semua standar yang berlaku. Sejak EC2-Classic jaringan Amazon dihentikan, instans Amazon Relational Database Service (Amazon RDS) tidak dapat lagi digunakan di luar VPC.	5 Juni 2026
Pembaruan untuk perekam terkait layanan CSPM	Menambahkan informasi terkait perekam konfigura si terkait layanan baru yang memungkinkan Security Hub CSPM melakukan pemeriksa an kontrol keamanan berdasarkan informasi konfigurasi sumber daya.	27 Mei 2026

Temuan akses yang tidak digunakan	Security Hub menambahkan fungsionalitas untuk menghasilkan dan menampilkan temuan akses yang tidak digunakan dari IAM Access Analyzer Mem ahami temuan akses yang tidak digunakan di Security Hub	Mei 19, 2026
Kontrol keamanan baru	Security Hub CSPM merilis lima kontrol baru. Beberapa kontrol mendukung standar F AWS oundational Security Best Practices (FSBP). Sebagian besar kontrol mendukung persyaratan NIST SP 800-53 Rev. 5. • Untuk standar AWS FSBP, ID untuk kontrol yang berlaku adalah: BedrockAgentCore.5 dan. BedrockAgentCore.6 • Untuk NIST SP 800-53 Rev. 5, ID untuk kontrol yang berlaku adalah: BedrockAgentCore.3,, BedrockAgentCore.4 dan. SageMaker.18	15 Mei 2026

Pembaruan untuk kebijakan terkelola - AWSSecurityHubServiceRolePolicy	Security Hub CSPM memperbarui kebijakan terkel AWS ola bernama. AWSSecurityHubServiceRolePolicy Pembaruan menambahkan izin untuk mengelola perekam konfigurasi terkait layanan Security Hub CSPM dan membuat peran terkait layanan. AWS Config	April 29, 2026
Kontrol keamanan baru	Security Hub CSPM merilis empat kontrol baru untuk standar F AWS oundational Security Best Practices (FSBP). Kontrol baru adalah: BedrockAgentCore.1, BedrockAgentCore.2, RDS.51, dan SageMaker.19.	April 22, 2026
Kontrol keamanan baru	Security Hub CSPM merilis lima kontrol baru untuk standar F AWS oundational Security Best Practices (FSBP). Kontrol baru adalah: APIGateway.11, EC2.183, EKS.9, SageMaker.16, dan SageMaker.17.	7 April 2026

Pembaruan standar dan kontrol keamanan	Kami menghentikan AppSync.6 kontrol AppSync.1 dan dan menghapusnya dari standar Praktik AWS Terbaik Keamanan Dasar (FSBP). AWS AppSync sekarang menyediakan enkripsi default pada semua cache API saat ini dan yang akan datang.	9 Maret, 2026
Pembaruan standar dan kontrol keamanan	Kami menghentikan ECS.1 kontrol dan menghapus kontrol dari standar Praktik Terbaik Keamanan AWS Dasar (FSBP) dan standar NIST SP 800-53 Rev. 5.	Maret 4, 2026
Kontrol keamanan baru	Security Hub CSPM merilis sebelas kontrol baru untuk standar F AWS oundation al Security Best Practices (FSBP). Kontrol baru adalah: APIGateway.10, ELB.21, ELB.22, RDS.50, SageMaker.9 SageMaker .10 SageMaker.11 SageMaker.12 SageMaker .13 SageMaker.14, dan SageMaker.15.	Februari 16, 2026

Pembaruan standar dan kontrol keamanan	Kami menghentikan MQ.3 kontrol dan menghapus kontrol dari semua standar yang berlaku. Kami menghentikan kontrol karena persyaratan Amazon MQ untuk peningkat an versi minor otomatis. Sebelumnya, kontrol ini diterapkan pada standar F AWS oundational Security Best Practices (FSBP), standar NIST SP 800-53 Rev. 5 dan standar PCI DSS v4.0.1. https://docs.aws. amazon.com/securityhub/ latest/userguide/pci-standa rd.html	Januari 12, 2026
Pembaruan untuk dokumenta si penaksir biaya	Menambahkan detail ke dokumentasi penaksir biaya Hub Keamanan tentang cara memberikan akses lintas akun untuk melakukan estimasi di akun selain akun manajemen.	Januari 12, 2026
Kontrol keamanan baru	Security Hub CSPM merilis lima kontrol baru untuk standar F AWS oundation al Security Best Practices (FSBP). Kontrol baru adalah: CloudFormation.4, CloudFron t.17, ECS.19, ECS.20, dan ECS.21.	Januari 6, 2026

Pembaruan standar dan kontrol keamanan	Karena persyaratan Amazon MQ untuk peningkatan versi minor otomatis, kami berencana untuk menghenti kan MQ.3 dan menghapus kontrol dari semua standar yang berlaku pada 12 Januari 2026. Saat ini, kontrol berlaku untuk standar F AWS oundational Security Best Practices (FSBP), standar NIST SP 800-53 Rev. 5 dan standar PCI DSS v4.0.1. https://docs.aws.amazon.com/securityhub/latest/userguide/pci-standard.html	Desember 12, 2025
Konten yang diperbarui untuk Service-Managed Standar: AWS Control Tower	Konten yang diperbarui untuk Service-Managed Standar: AWS Control Tower untuk memberikan panduan yang lebih baik untuk membuat, melihat, dan menonaktifkan kontrol dalam standar dari AWS Control Tower.	Desember 8, 2025
Kontrol keamanan baru	Security Hub CSPM merilis tujuh kontrol baru untuk standar F AWS oundation al Security Best Practices (FSBP). Kontrol baru adalah: Cognito.4, Cognito.5 , Cognito.6, EC2.182 CloudFormation.3, ECS.18, dan SES.3.	Desember 8, 2025

Konten yang diperbarui untuk Ketersediaan Umum Hub Keamanan	Menambahkan konten untuk mendukung rilis Ketersedi aan Umum dari Hub AWS Keamanan	Desember 2, 2025
Konten yang diperbarui untuk Security Hub	Menambahkan konten untuk Tren, dan Agregasi Wil ayah. Perubahan ini mendukung rilis pratinjau Hub Keamanan.	November 21, 2025
Pembaruan untuk kebijakan terkelola - `AWSSecuri tyHubV2ServiceRole Policy`	Security Hub memperbarui kebijakan ter AWS kelola bernama`AWSSecuri tyHubV2ServiceRole Policy` . Pembaruan menambahkan kemampuan pengukuran untuk Amazon Elastic Container Registry AWS Lambda,, Amazon CloudWatch, dan AWS Identity and Access Managemen t untuk mendukung fitur Security Hub. Pembaruan juga menambahkan dukungan untuk AWS Config pe rekam global. Perubahan ini mendukung rilis pratinjau Hub Keamanan.	November 17, 2025

Pembaruan untuk kebijakan terkelola - AWSSecurityHubOrganizationsAccess	Security Hub memperbarui kebijakan ter AWS kelola bernamaAWSSecurityHubOrganizationsAccess . Pembaruan menambahkan izin untuk menjelaskan kebijakan sumber daya yang mendukung fitur Hub Keamanan. Perubahan ini mendukung rilis pratinjau Hub Keamanan.	November 17, 2025
Pembaruan untuk kebijakan terkelola - AWSSecurityHubFullAccess	Security Hub memperbarui kebijakan ter AWS kelola bernamaAWSSecurityHubFullAccess . Pembaruan menambahkan kemampuan seputar pengelolaan GuardDuty, Amazon Inspector, dan manajemen akun untuk mendukung fitur Hub Keamanan. Perubahan ini mendukung rilis pratinjau Hub Keamanan.	November 17, 2025
Pembaruan untuk kontrol keamanan	Kami mengubah tingkat keparahan 10 kontrol CSPM Security Hub: CloudFront.7, CloudTrail.5, ELB.7,, GuardDuty.7, MQ.3, Opensearch.10, RDS.7 ServiceCatalog.1 SNS.4, dan. SQS.3 Untuk rincian perubahan, lihat Log perubahan untuk kontrol CSPM Hub Keamanan.	November 13, 2025

Kontrol keamanan baru	Security Hub CSPM merilis enam kontrol baru untuk standar F AWS oundation al Security Best Practices (FSBP). Kontrol baru adalah: Cognito.3, DMS.13, EC2.181, RDS.43, RDS.47, dan RDS.48.	Oktober 28, 2025
Standar keamanan baru	Security Hub CSPM sekarang menyediakan standar keamanan yang selaras dengan CIS Foun dations Benchmark v5.0.0 AWS . Standar baru ini mencakup 40 kontrol keamanan yang ada. Kontrol melakukan pemeriksa an otomatis yang mengevalu asi sumber daya tertentu untuk kepatuhan dengan subset persyaratan yang ditentukan oleh kerangka kerja.	Oktober 16, 2025
Integrasi pihak ketiga baru	Elasticadalah integrasi pihak ketiga baru yang dapat menerima temuan dari Security Hub CSPM.	3 Oktober 2025

Pembaruan standar dan kontrol keamanan	Kami menghentikan RedshiftServerless.7 kontrol Redshift.9 dan dan menghapusnya dari semua standar yang berlaku. Kami menghentikan kontrol ini karena keterbatasan Amazon Redshift yang melekat yang mencegah remediasi `FAILED` temuan yang efektif untuk kontrol. Sebelumnya, kontrol ini diterapkan pada standar F AWS oundational Security Best Practices (FSBP) dan standar NIST SP 800-53 Rev. 5. Redshift.9 Kontrol juga diterapkan pada standar yang AWS Control Tower dikelola layanan.	September 24, 2025
Ketersediaan regional	Security Hub CSPM sekarang tersedia di Wilayah Asia Pasifik (Selandia Baru). Untuk daftar lengkap Wilayah AWS tempat CSPM Security Hub saat ini tersedia, lihat titik akhir dan kuota Hub AWS Keamanan di. Referensi Umum AWS	September 19, 2025
Kontrol keamanan baru	Security Hub CSPM merilis dua kontrol baru untuk standar F AWS oundational Security Best Practices (FSBP): dan. CloudFront.16 RDS.46	3 September 2025

Ketersediaan regional	Standar AWS Resource Tagging sekarang tersedia di Wilayah Asia Pasifik (Thailand) dan Meksiko (Tengah).	Agustus 29, 2025
Pembaruan standar dan kontrol keamanan	Karena keterbatasan Amazon Redshift, kami berencana untuk menghentikan RedshiftS erverless.7 kontrol Redshift. 9 dan dan menghapusnya dari semua standar yang berlaku pada 15 September 2025. Saat ini, kontrol ini berlaku untuk standar F AWS oundational Security Best Practices (FSBP) dan standar NIST SP 800-53 Rev. 5. Redshift.9 Kontrol juga berlaku untuk standar yang AWS Control Tower dikelola layanan.	Agustus 15, 2025
Objek detail sumber daya baru di ASFF	AWS Security Finding Format (ASFF) sekarang menyertak an objek sumber `CodeRepos itory` daya. Objek ini memberikan detail tentang repositori kode eksternal yang Anda sambungkan ke AWS sumber daya dan mengonfig urasi Amazon Inspector untuk memindai kerentanan.	Agustus 1, 2025

Ketersediaan regional	Security Hub CSPM sekarang tersedia di Wilayah Asia Pasifik (Taipei). Untuk daftar lengkap Wilayah AWS tempat CSPM Security Hub saat ini tersedia, lihat titik akhir dan kuota Hub AWS Keamanan di. Referensi Umum AWS	Juli 23, 2025
Integrasi pihak ketiga baru	Dynatraceadalah integrasi pihak ketiga baru yang dapat menerima temuan dari Security Hub CSPM.	Juli 18, 2025
Kontrol keamanan baru	Security Hub CSPM merilis 13 kontrol baru. Sebagian besar kontrol mendukung standar F AWS oundation al Security Best Practices (FSBP). Beberapa kontrol mendukung persyaratan NIST SP 800-53 Rev. 5. • Untuk standar AWS FSBP, ID untuk kontrol yang berlaku adalah: CloudFron t.15,, Cognito.2, EC2.180, ELB.18, MSK.4, MSK.5, MSK.6, RDS.45, Redshift. 18 S3.25 SSM.6, dan. SSM.7 • Untuk NIST SP 800-53 Rev. 5, ID untuk kontrol yang berlaku adalah: dan. Lambda.7 RDS.45	Juli 15, 2025

Pembaruan untuk pembuatan temuan kontrol	Untuk membantu Anda melacak perubahan kepatuhan , Security Hub CSPM sekarang memperbarui temuan kontrol yang ada, alih-alih menghasilkan temuan baru, ketika ada perubahan pada status kepatuhan sumber daya individu. Ini berarti Anda dapat menggunakan data yang disediakan oleh temuan individual untuk melacak perubahan kepatuhan untuk sumber daya tertentu terhadap kontrol tertentu.	Juli 3, 2025
Pembaruan standar dan kontrol keamanan	Kami menghapus IAM.13 kontrol dari standar PCI DSS v4.0.1. Kami juga menghapus IAM.17 kontrol dari standar NIST SP 800-171 Revisi 2. Standar tidak secara eksplisit memerlukan pemeriksaan yang disediakan kontrol ini. Kami juga memperbar ui detail persyaratan terkait untuk standar ini untuk kontrol tertentu yang memeriksa kebijakan kata sandi IAM: IAM.7, dan seterusnya IAM.10 . IAM.17	Juni 30, 2025

Pembaruan untuk menemukan retensi	Security Hub CSPM sekarang menyimpan temuan yang diarsipkan selama 30 hari, bukan 90 hari, yang dapat mengurangi kebisingan pencarian. Untuk retensi jangka panjang, Anda dapat mengekspor temuan ke bucket S3 dengan menggunakan tindakan kustom dengan aturan Amazon EventBridge .	Juni 20, 2025
Pembaruan untuk kebijakan terkelola yang ada	Security Hub CSPM menambahkan izin baru ke kebijakan terkel AWS ola bernama. `AWSSecurityHubOrganizationsAccess` Izin tersebut memungkinkan manajemen organisasi untuk mengaktifkan dan mengelola Security Hub dan Security Hub CSPM dalam organisasi. Security Hub CSPM juga menambahkan izin baru ke kebijakan terkel AWS ola bernama. `AWSSecurityHubFullAccess` Izin ini memungkinkan kepala sekolah untuk membuat peran terkait layanan untuk Hub Keamanan.	Juni 18, 2025

Rilis pratinjau publik dan kebijakan terkelola baru untuk Security Hub	Rilis pratinjau publik dari AWS Security Hub dan Panduan Pengguna Hub Keamanan . AWS Rilis ini mencakup kebijakan ter AWS kelola baru,`AWSSecurityHubV2ServiceRolePolicy` . Kebijakan ini memungkinkan Hub Keamanan untuk mengelola AWS Config aturan dan sumber daya Hub Keamanan di organisasi pelanggan dan atas nama pelanggan. Security Hub dalam rilis pratinjau dan dapat berubah.	Juni 17, 2025
Pembaruan standar dan kontrol keamanan	Kami menghapus IAM.10 kontrol dari standar PCI DSS v4.0.1. Kontrol ini memeriksa apakah kebijakan kata sandi akun untuk pengguna IAM memenuhi persyaratan minimum, termasuk panjang kata sandi minimum 7 karakter. PCI DSS v4.0.1 sekarang membutuhkan kata sandi untuk memiliki minimal 8 karakter. IAM.10 Kontrol terus berlaku untuk standar PCI DSS v3.2.1, yang memiliki persyaratan kata sandi berbeda.	30 Mei 2025

Standar keamanan baru	Security Hub CSPM sekarang menyediakan standar keamanan yang selaras dengan kerangka kerja keamanan siber dan kepatuhan NIST SP 800-171 Revisi 2. Standar baru ini mencakup lebih dari 60 kontrol keamanan yang ada. Kontrol melakukan pemeriksaan otomatis yang mengevaluasi tertentu Layanan AWS dan sumber daya untuk kepatuhan dengan subset persyaratan yang ditentukan oleh kerangka kerja.	29 Mei 2025
Pembaruan untuk kontrol keamanan	Security Hub CSPM mengembalikan rilis kontrol berikut di semua Wilayah AWS: [RDS.46] Instans DB RDS tidak boleh digunakan di subnet publik dengan rute ke gateway internet. Sebelumnya, kontrol ini mendukung standar F AWS oundation al Security Best Practices (FSBP).	8 Mei 2025

Kontrol keamanan baru	Security Hub CSPM merilis 9 kontrol baru. Sebagian besar kontrol mendukung standar F AWS oundational Security Best Practices (FSBP). Beberapa kontrol mendukung persyaratan NIST SP 800-53 Rev. 5. • Untuk standar AWS FSBP, ID untuk kontrol yang berlaku adalah: DocumentDB.6,,, RDS.44, RedshiftServerless.2, RedshiftServerless.3 RedshiftServerless.5 RedshiftServerless.6, dan RedshiftServerless.7 (kemudian dihentikan). • Untuk NIST SP 800-53 Rev. 5, ID untuk kontrol yang berlaku adalah: CloudTrail.10, RedshiftServerless.4, dan RedshiftServerless.7 (kemudian dihentikan).	7 Mei 2025

Kontrol keamanan baru	Security Hub CSPM merilis 24 kontrol baru. Sebagian besar kontrol mendukung F AWS oundational Security Best Practices (FSBP) atau standar AWS Resource Tagging. Beberapa kontrol mendukung persyaratan NIST SP 800-53 Rev. 5. • Untuk standar AWS FSBP, ID untuk kontrol yang berlaku adalah: EC2.173,, RDS.41 RDS.42, dan. SageMaker.8 • Untuk standar AWS Penandaan Sumber Daya, ID untuk kontrol yang berlaku adalah: Amplify.1 , Amplify.2, Batch.4, DataSync.2, EC2.174, EC2.175, EC2.176, EC2.177, EC2.178, EC2.179, Redshift.17, SageMaker.6, SageMaker .7 SSM.5, Transfer.4, Transfer.5, Transfer.6, dan Transfer.7. • Untuk NIST SP 800-53 Rev. 5, ID untuk kontrol yang berlaku adalah: dan. ECS.17 RDS.42	April 16, 2025

Kontrol keamanan baru	Security Hub CSPM merilis empat kontrol baru untuk standar Praktik AWS Terbaik Keamanan Dasar. Kontrolnya adalah: • the section called “[FSx.3] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk penerapan Multi-AZ” • the section called “[FSx.4] fsX untuk sistem file NetApp ONTAP harus dikonfigurasi untuk penerapan Multi-AZ” • the section called “[FSx.5] Sistem file FSx for Windows File Server harus dikonfigurasi untuk penyebaran Multi-AZ” • the section called “[RedshiftServerless.1] Grup kerja Amazon Redshift Tanpa Server harus menggunakan perutean VPC yang disempurnakan”	Maret 18, 2025

Pembaruan standar dan kontrol keamanan	Kami menghapus kontrol RDS.18 keamanan (kemudian pensiun) dari standar Praktik AWS Terbaik Keamanan Dasar dan pemeriksaan otomatis untuk persyaratan NIST SP 800-53 Rev. 5. Sejak EC2-Classic jaringan Amazon dihentikan, instans Amazon Relational Database Service (Amazon RDS) tidak dapat lagi digunakan di luar VPC.	Maret 7, 2025
Pembaruan untuk temuan kontrol	Security Hub CSPM sekarang menghasilkan `WARNING` temuan untuk kontrol yang diaktifkan jika perekaman https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-setup-prereqs.html#config-resource-recording sumber daya tidak diaktifkan AWS Config untuk jenis sumber daya yang diperiksa kontrol. Ini dapat membantu Anda mengidentifikasi dan mengatasi potensi celah konfigurasi dalam pemeriksaan kontrol keamanan Anda.	Februari 25, 2025

Kontrol keamanan baru	Security Hub CSPM merilis 11 kontrol baru. Kontrolnya adalah: • the section called “[Connect .2] Connect Instans Pelanggan seharusnya mengaktifkan CloudWatch pencatatan” • the section called “[ECR.5] Repositori ECR harus dienkripsi dengan yang dikelola pelanggan AWS KMS keys” • the section called “[ELB.17] Penyeimbang Beban Aplikasi dan Jaringan dengan pendengar harus menggunakan kebijakan keamanan yang direkomen dasikan” • the section called “[Glue.4] AWS GluePekerjaan percikan harus berjalan pada versi yang didukungA WS Glue” • the section called “[GuardDu ty.11] GuardDuty Runtime Monitoring harus diaktifkan” • the section called “[GuardDu ty.12] GuardDuty ECS Runtime Monitoring harus diaktifkan” • the section called “[GuardDu ty.13] GuardDuty EC2	Februari 24, 2025

Runtime Monitoring harus diaktifkan”

- the section called “[Network Firewall.10] Firewall Firewall Jaringan harus mengaktifkan perlindungan perubahan subnet”
- the section called “[RDS.40] RDS untuk instans SQL Server DB harus menerbitkan log ke Log CloudWatch”
- the section called “[SQS.3] Kebijakan akses antrian SQS seharusnya tidak mengizinkan akses publik”
- the section called “[Transfer.3] Konektor Transfer Family seharusnya mengaktifkan logging”

Kontrol keamanan baru	Security Hub CSPM merilis 37 kontrol baru untuk Standar Penandaan AWS Sumber Daya. Security Hub CSPM juga merilis kontrol baru berikut: • the section called “[EMR.3] Konfigurasi keamanan Amazon EMR harus dienkripsi saat istirahat” • the section called “[EMR.4] Konfigurasi keamanan Amazon EMR harus dienkripsi saat transit” • the section called “[SageMaker.5] SageMaker model harus mengaktifkan isolasi jaringan”	Januari 22, 2025
Kontrol keamanan baru	Security Hub CSPM merilis EC2.172 EC2 VPC Block Pengaturan Akses Publik harus memblokir lalu lintas gateway internet.	Januari 15, 2025

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia. • the section called “[Cognito .1] Kumpulan pengguna Cognito harus mengaktif kan perlindungan ancaman dengan mode penegakan fungsi penuh untuk otentikas i standar” • the section called “[RDS.38] RDS untuk instans DB PostgreSQL harus dienkrips i saat transit” • the section called “[RDS.39] RDS untuk instans MySQL DB harus dienkripsi saat transit” • the section called “[Redshif t.16] Grup subnet cluster Redshift harus memiliki subnet dari beberapa Availability Zone”	Desember 17, 2024
Hub Keamanan CSPM mendukung PCI DSS v4.0.1	Security Hub CSPM sekarang mendukung v4.0.1 dari Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS). Untuk informasi selengkapnya tentang standar dan kontrol yang berlaku untuk itu, lihat PCI DSS di Security Hub C SPM.	Desember 11, 2024

Security Hub CSPM menerima temuan urutan GuardDuty serangan	Security Hub CSPM sekarang menerima temuan urutan serangan dari Amazon GuardDuty Extended Threat Detection. Detail pencarian urutan serangan tersedia di objek Deteksi dari Format Penem AWS uan Keamanan (ASFF).	Desember 1, 2024
Security Hub CSPM didukung di yang baru Wilayah AWS	Security Hub CSPM sekarang tersedia di Wilayah Asia Pasifik (Malaysia). Beberapa kontrol keamanan memiliki keterbatasan Regional. Untuk daftar kontrol yang tidak tersedia di Wilayah ini, lihat Batas regional pada kontrol CSPM Hub Keamanan.	November 22, 2024
Perubahan ke Config.1	Security Hub CSPM meningkatkan tingkat keparahan Config.1 kontrol dari `MEDIUM` ke`CRITICAL`, dan menambahkan kode status baru dan alasan status untuk temuan yang gagal Config.1 . Untuk informasi selengkapnya tentang perubahan, lihat entri untuk 20 November 2024 di Log perubahan untuk kontrol CSPM Security Hub.	20 November 2024

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia. Kontrol ini adalah bagian dari Prakti AWS k Terbaik Keamanan Dasar dan NIST SP 800-53 Rev. 5, dan mereka mengevaluasi apakah cloud pribadi virtual (VPC) yang Anda kelola memiliki titik akhir VPC antarmuka untuk sumber daya atau. Layanan AWS AWS • the section called “[EC2.55] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk ECR API” • the section called “[EC2.56] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Docker Registry” • the section called “[EC2.57] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Systems Manager” • the section called “[EC2.58] VPC harus dikonfigurasi dengan titik akhir antarmuka untuk Kontak Manajer Insiden Manajer Systems Manager” • the section called “[EC2.60] VPC harus dikonfigurasi dengan titik akhir antarmuka	15 November 2024

	untuk Systems Manager Incident Manager”	
Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia. • the section called “[AppSync .1]AWS AppSyncCache API harus dienkripsi saat istirahat” • the section called “[AppSync .6]AWS AppSyncCache API harus dienkripsi saat transit” • the section called “[EC2.170] Template peluncuran EC2 harus menggunakan Layanan Metadata Instans Versi 2 (IMDSv2)” • the section called “[EC2.171] Koneksi VPN EC2 seharusnya mengaktifkan logging” • the section called “[EFS.8] Sistem file EFS harus dienkripsi saat diam” • the section called “[KMS.5] Kunci KMS tidak boleh diakses publik” • the section called “[SNS.4] Kebijakan akses topik SNS seharusnya tidak mengizink an akses publik”	Oktober 18, 2024

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia. • the section called “[ECS.16] Kumpulan tugas ECS seharusnya tidak secara otomatis menetapkan alamat IP publik” • the section called “[GuardDuty.7] GuardDuty EKS Runtime Monitoring harus diaktifkan” • the section called “[Kinesis.3] Aliran Kinesis harus memiliki periode retensi data yang memadai” • the section called “[MSK.3] Konektor MSK Connect harus dienkripsi saat transit” • the section called “[RDS.36] RDS untuk instans DB PostgreSQL harus menerbitkan log ke Log CloudWatch” • the section called “[RDS.37] Cluster DB Aurora PostgreSQL harus menerbitkan log ke Log CloudWatch” • the section called “[S3.24] S3 Multi-Region Access Points harus mengaktifkan pengaturan akses publik blok”	3 Oktober 2024

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia. • the section called “[Athena.4] Kelompok kerja Athena seharusnya mengaktifkan pencatatan” • the section called “[CodeBuild.7] ekspor kelompok CodeBuild laporan harus dienkripsi saat istirahat” • the section called “[DataSync.1] DataSync tugas harus mengaktifkan logging” • the section called “[EFS.7] Sistem file EFS harus mengaktifkan cadangan otomatis” • Glue.2 (pensiun) • the section called “[Glue.3] AWS Gluetransformasi pembelajaran mesin harus dienkripsi saat istirahat” • the section called “[WorkSpaces.1] volume WorkSpaces pengguna harus dienkripsi saat istirahat” • the section called “[WorkSpaces.2] volume WorkSpaces root harus dienkripsi saat istirahat”	Agustus 30, 2024

Panel temuan baru	Panel penemuan baru di konsol CSPM Security Hub membantu Anda dengan cepat mengambil tindakan terhadap temuan, meninjau detail sumber daya dan menemukan riwayat, dan menemukan informasi terkait lainnya tentang temuan.	Agustus 16, 2024
Perbarui untuk Config.1 mengontrol	Config.1Kontrol memeriksa apakah AWS Config diaktifkan, menggunakan peran terkait layanan, dan merekam sumber daya untuk kontrol yang diaktifkan. Security Hub CSPM menambahkan parameter kontrol khusus bernama. `includeConfigServiceLinkedRoleCheck` Dengan menyetel parameter ini ke`false`, Anda dapat memilih untuk tidak memeriksa apakah AWS Config menggunakan peran yang ditautkan layanan.	Agustus 15, 2024
Tentukan Wilayah rumah tanpa Wilayah tertaut	Anda sekarang dapat membuat agregator pencarian dan membangun Wilayah rumah tanpa menghubungkan apa pun Wilayah AWS ke Wilayah asal. Ini memungkinkan Anda untuk mengaktifkan konfigurasi pusat tanpa menentukan Wilayah tertaut.	Juli 25, 2024

Pilih kontrol yang tersedia di lebih banyak Wilayah	Kontrol berikut sekarang tersedia dalam tambahan Wilayah AWS, termasuk AS Timur (Virginia Utara) dan AS Timur (Ohio). • the section called “[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat” • the section called “[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM” • the section called “[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi” • the section called “[DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS” • the section called “[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit” • the section called “[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan” • the section called “[EKS.3] Cluster EKS harus	Juli 15, 2024

menggunakan rahasia Kubernetes terenkripsi”

- the section called “[FSx.2] Sistem file FSx for Lustre harus dikonfigurasi untuk menyalin tag ke cadangan”
- the section called “[MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch”
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- the section called “[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus”
- the section called “[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi”
- the section called “[SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1”
- the section called “[Service Catalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja”

- the section called “[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir”

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia: • the section called “[GuardDuty.5] Pemantauan Log Audit GuardDuty EKS harus diaktifkan” • the section called “[GuardDuty.6] Perlindungan GuardDuty Lambda harus diaktifkan” • the section called “[GuardDuty.8] Perlindungan GuardDuty Malware untuk EC2 harus diaktifkan” • the section called “[GuardDuty.9] Perlindungan GuardDuty RDS harus diaktifkan” • the section called “[GuardDuty.10] Perlindungan GuardDuty S3 harus diaktifkan” • the section called “[Inspector.1] Pemindaian Amazon Inspector EC2 harus diaktifkan” • the section called “[Inspector.2] Pemindaian ECR Amazon Inspector harus diaktifkan” • the section called “[Inspector.3] Pemindaian kode Amazon Inspector Lambda harus diaktifkan”	Juli 11, 2024

- the section called “[Inspector.4] Pemindaian standar Amazon Inspector Lambda harus diaktifkan”

Rilis CIS Foun AWS dations Benchmark v3.0.0	Security Hub CSPM merilis Center for Internet Security (CIS) Foun AWS dations Benchmark v3.0.0. Rilis ini mencakup kontrol baru berikut, serta pemetaan ke beberapa kontrol yang ada. • the section called “[EC2.53] Grup keamanan EC2 seharusnya tidak mengizinkan masuknya dari 0.0.0. 0/0 ke port administrasi server jarak jauh” • the section called “[EC2.54] Grup keamanan EC2 tidak boleh mengizinkan masuknya dari: :/0 ke port administrasi server jarak jauh” • the section called “[IAM.26] SSL/TLS Sertifikat kedaluwarsa yang dikelola di IAM harus dihapus” • the section called “[IAM.27] Identitas IAM seharusnya tidak memiliki kebijakan yang dilampirkan AWSCloudShellFullAccess” • the section called “[IAM.28] IAM Access Analyzer penganalisis akses eksternal harus diaktifkan” • the section called “[S3.22] Bucket tujuan umum S3	Mei 13, 2024

harus mencatat peristiwa penulisan tingkat objek”

- the section called “[S3.23] Bucket tujuan umum S3 harus mencatat peristiwa baca tingkat objek”

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia: • the section called “[DataFirehose.1] Aliran pengiriman Firehose harus dienkripsi saat istirahat” • the section called “[DMS.10] Titik akhir DMS untuk database Neptunus harus mengaktifkan otorisasi IAM” • the section called “[DMS.11] Titik akhir DMS untuk MongoDB harus mengaktifkan mekanisme otentikasi” • the section called “[DMS.12] Titik akhir DMS untuk Redis OSS seharusnya mengaktifkan TLS” • the section called “[DynamoDB.7] Cluster DynamoDB Accelerator harus dienkripsi saat transit” • the section called “[EFS.6] Target pemasangan EFS tidak boleh dikaitkan dengan subnet yang menetapkan alamat IP publik saat diluncurkan” • the section called “[EKS.3] Cluster EKS harus menggunakan rahasia Kubernetes terenkripsi” • the section called “[FSx.2] Sistem file FSx for Lustre	3 Mei 2024

harus dikonfigurasi untuk menyalin tag ke cadangan”

- the section called “[MQ.2] Pialang ActiveMQ harus mengalirkan log audit ke CloudWatch”
- [MQ.3] Broker Amazon MQ harus mengaktifkan peningkatan versi minor otomatis
- the section called “[Opensearch.11] OpenSearch domain harus memiliki setidaknya tiga node primer khusus”
- the section called “[Redshift.15] Grup keamanan Redshift harus mengizinkan masuknya port cluster hanya dari asal yang dibatasi”
- the section called “[SageMaker.4] SageMaker varian produksi titik akhir harus memiliki jumlah instance awal lebih besar dari 1”
- the section called “[Service Catalog.1] Portofolio Service Catalog harus dibagikan dalamAWSorganisasi saja”
- the section called “[Transfer.2] Server Transfer Family tidak boleh menggunakan protokol FTP untuk koneksi titik akhir”

AWS Standar Penandaan Sumber Daya	Standar AWS Penandaan Sumber Daya dari Security Hub CSPM sekarang tersedia secara umum, bersama dengan kontrol baru yang berlaku untuk standar.	30 April 2024
Perbarui ke kebijakan terkelola yang ada	Security Hub CSPM memperbarui kebijakan ter AWS kelola bernama `AmazonSecurityHubFullAccess` untuk mendapatkan detail harga untuk Layanan AWS dan produk.	April 24, 2024
In-context konfigurasi parameter kontrol	Jika Anda menggunakan konfigurasi pusat, Anda sekarang dapat mengonfigurasi parameter kontrol dalam konteks, dari halaman detail kontrol pada konsol CSPM Security Hub.	Maret 29, 2024
Perbarui ke kebijakan terkelola yang ada	Security Hub CSPM memperbarui kebijakan terkel AWS ola yang `Sid` diberi nama `AWSSecurityHubReadOnlyAccess` dengan menambahkan bidang.	Februari 22, 2024

Kontrol keamanan baru	Kontrol [Macie.2] Penemuan data sensitif otomatis Macie harus diaktifkan sekarang tersedia. Untuk batasan regional pada kontrol ini, lihat Keter sediaan kontrol berdasarkan Wilayah.	Februari 19, 2024
Security Hub CSPM tersedia di Kanada Barat (Calgary)	Security Hub CSPM sekarang tersedia di Kanada Barat (Calgary). Semua fitur CSPM Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat Ketersediaan kontrol menurut Wilayah.	20 Desember 2023

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia: • the section called “[Backup.1]AWS Backuptitik pemulihan harus dienkripsi saat istirahat” • the section called “[DynamoDB.6] Tabel DynamoDB harus mengaktifkan perlindungan penghapusan” • the section called “[EC2.51] Titik akhir EC2 Client VPN harus mengaktifkan pencatatan koneksi klien” • the section called “[EKS.8] Cluster EKS harus mengaktifkan logging audit” • the section called “[EMR.2] Pengaturan akses publik blok EMR Amazon harus diaktifkan” • the section called “[FSx.1] FSx untuk sistem file OpenZFS harus dikonfigurasi untuk menyalin tag ke cadangan dan volume” • the section called “[Macie.1] Amazon Macie harus diaktifkan” • the section called “[MSK.2] Kluster MSK seharusnya memiliki pemantauan yang	14 Desember 2023

ditingkatkan yang dikonfigu rasi”

- the section called “[Neptune .9] Cluster DB Neptunus harus digunakan di beberapa Availability Zone”
- the section called “[Network Firewall.1] Firewall Firewall Jaringan harus digunakan di beberapa Availability Zone”
- the section called “[Network Firewall.2] Pencatatan Firewall Jaringan harus diaktifkan”
- the section called “[Opensea rch.10] OpenSearch domain harus menginstal pembaruan perangkat lunak terbaru”
- the section called “[PCA.1]A WS Private CAotorita s sertifikat root harus dinonaktifkan”
- the section called “[S3.19] Titik akses S3 harus mengaktifkan pengaturan akses publik blok”
- the section called “[S3.20] Bucket tujuan umum S3 harus mengaktifkan penghapusan MFA”

Menemukan pengayaan	Security Hub CSPM menambahkan bidang temuan baru`AwsAccoun tName` ,`ApplicationArn` , dan `ApplicationName` ke AWS Security Finding Format (ASFF).	27 November 2023
Peningkatan pada dasbor Ringkasan	Anda sekarang dapat mengakses lebih banyak widget dasbor di halaman Ring kasan konsol CSPM Hub Keamanan, menyimpan set filter dasbor untuk fokus dengan cepat pada masalah keamanan tertentu, dan menyesuaikan tata letak dasbor.	27 November 2023
Konfigurasi pusat	Konfigurasi pusat sekarang tersedia. Dengan konfigura si pusat, administrator yang didelegasikan oleh Security Hub CSPM dapat mengonfig urasi Security Hub CSPM, standar, dan kontrol di beberapa akun organisasi, unit organisasi (OU), dan Wilayah.	27 November 2023

Pembaruan untuk kebijakan terkelola	Security Hub CSPM menambahkan izin baru ke kebijakan terkel `AWSSecurityHubServiceRolePolicy` ola yang memungkinkan Security Hub CSPM membaca dan memperbarui properti kontrol keamanan yang dapat disesuaikan.	26 November 2023
Parameter kontrol kustom	Anda sekarang dapat menyesuaikan nilai parameter untuk kontrol CSPM Security Hub tertentu. Ini dapat membuat temuan untuk kontrol tertentu lebih relevan dengan persyaratan bisnis dan harapan keamanan Anda.	26 November 2023
Pembaruan kebijakan terkelola	Security Hub CSPM memperbarui `AWSSecurityHubFullAccess` dan `AWSSecurityHubOrganizationsAccess` mengelola kebijakan yang memungkinkan Anda untuk menggunakan, masing-masing, fitur CSPM Security Hub dan integrasi dengan. AWS Organizations	16 November 2023

Kontrol keamanan yang ada ditambahkan ke Service-Managed Standar: AWS Control Tower	Kontrol CSPM Hub Keamanan yang ada berikut telah ditambahkan ke Service-Managed Standar:. AWS Control Tower • ACM.2 • AppSync.5 • CloudTrail.6 • DMS.9 • DocumentDB.3 • DynamoDB.3 • EC2.23 • EKS.1 • ElastiCache.3 • ElastiCache.4 • ElastiCache.5 • ElastiCache.6 • EventBridge.3 • KMS.4 • Lambda.3 • MQ.5 • MQ.6 • MSK.1 • RDS.12 • RDS.15 • S3.17	14 November 2023

Pembaruan untuk kebijakan terkelola	Security Hub CSPM menambahkan izin penandaan baru ke kebijakan terkel `AWSSecurityHubServiceRolePolicy` ola yang memungkinkan Security Hub CSPM membaca tag sumber daya yang terkait dengan temuan.	7 November 2023

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia: • the section called “[AppSync .5]AWS AppSyncGraphQL API tidak boleh diautentikasi dengan kunci API” • the section called “[DMS.6] Instans replikasi DMS harus mengaktifkan peningkatan versi minor otomatis” • the section called “[DMS.7] Tugas replikasi DMS untuk basis data target harus mengaktifkan logging” • the section called “[DMS.8] Tugas replikasi DMS untuk basis data sumber harus mengaktifkan logging” • the section called “[DMS.9] Titik akhir DMS harus menggunakan SSL” • the section called “[DocumentDB.3] Cuplikan cluster manual Amazon DocumentDB seharusnya tidak bersifat publik” • the section called “[DocumentDB.4] Cluster Amazon DocumentDB harus mempublikasikan log audit ke Log CloudWatch” • the section called “[DocumentDB.5] Cluster Amazon DocumentDB harus	10 Oktober 2023

mengaktifkan perlindungan penghapusan”

- the section called “[ECS.9] Definisi tugas ECS harus memiliki konfigurasi logging”
- the section called “[EventBridge.3] bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir”
- the section called “[EventBridge.4] titik akhir EventBridge global harus mengaktifkan replikasi acara”
- the section called “[MSK.1] Cluster MSK harus dienkripsi dalam perjalanan di antara node broker”
- the section called “[MQ.5] Broker ActiveMQ harus menggunakan mode penerapan active/standby”
- the section called “[MQ.6] Broker RabbitMQ harus menggunakan mode penerapan cluster”
- the section called “[Network Firewall.9] Firewall Firewall Jaringan harus mengaktifkan perlindungan penghapusan”
- the section called “[RDS.34] Cluster Aurora MySQL DB harus menerbitkan log audit ke CloudWatch Log”

	• the section called “[RDS.35] Cluster RDS DB harus mengaktifkan peningkatan versi minor otomatis” • the section called “[Route53 .2] Rute 53 zona yang dihosting publik harus mencatat kueri DNS” • the section called “[WAF.12] AWS WAFaturan harus mengaktifkan CloudWatch metrik”	
Pembaruan untuk kebijakan terkelola	Security Hub CSPM menambahkan tindakan Organisasi baru ke kebijakan terkel `AWSSecuri tyHubServiceRolePo licy` ola yang memungkin kan Security Hub CSPM mengambil informasi akun dan unit organisasi (OU). Kami juga menambahkan tindakan CSPM Security Hub baru yang memungkinkan Security Hub CSPM membaca dan memperbarui konfigurasi layanan, termasuk standar dan kontrol.	27 September 2023

Kontrol keamanan yang ada ditambahkan ke Service-Managed Standar: AWS Control Tower	Kontrol CSPM Hub Keamanan yang ada berikut telah ditambahkan ke Service-Managed Standar:. AWS Control Tower • the section called “[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat” • the section called “[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat” • the section called “[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai” • the section called “[Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat” • the section called “[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch” • the section called “[Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik” • the section called “[Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan”	26 September 2023

- the section called “[Neptune .5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis”
- the section called “[Neptune .6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat”
- the section called “[Neptune .7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM”
- the section called “[Neptune .8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot”
- the section called “[RDS.27] Cluster RDS DB harus dienkripsi saat diam”

Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi tersedia di AWS GovCloud (US)	Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi sekarang tersedia di AWS GovCloud (US) Region. Halaman Kontrol pada konsol CSPM Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Saat Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.	September 6, 2023
Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi tersedia di Wilayah China	Tampilan kontrol konsolidasi dan temuan kontrol konsolidasi sekarang tersedia di Wilayah China. Halaman Kontrol pada konsol CSPM Security Hub menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Saat Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.	28 Agustus 2023

Security Hub CSPM tersedia di Wilayah Israel (Tel Aviv)	Security Hub CSPM sekarang tersedia di Israel (Tel Aviv). Semua fitur CSPM Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat Ketersediaan kontrol menurut Wilayah.	8 Agustus 2023

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia: • the section called “[Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat” • the section called “[DocumentDB.1] Cluster Amazon DocumentDB harus dienkripsi saat istirahat” • the section called “[DocumentDB.2] Cluster Amazon DocumentDB harus memiliki periode retensi cadangan yang memadai” • the section called “[Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat” • the section called “[Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch” • the section called “[Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik” • the section called “[Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan” • the section called “[Neptune.5] Cluster DB Neptunus	28 Juli 2023

	harus mengaktifkan cadangan otomatis” • the section called “[Neptune .6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat” • the section called “[Neptune .7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM” • the section called “[Neptune .8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot” • the section called “[RDS.27] Cluster RDS DB harus dienkripsi saat diam”	
Operator baru untuk kriteria aturan otomatisasi	Anda sekarang dapat menggunakan operator perbandingan CONTAINS dan NOT_CONTAINS untuk peta aturan otomatisasi dan kriteria string.	25 Juli 2023
Aturan otomatisasi	Security Hub CSPM sekarang menawarkan aturan otomatisasi yang secara otomatis memperbarui temuan berdasarkan kriteria yang Anda tentukan.	13 Juni 2023
Integrasi pihak ketiga baru	Snykadalah integrasi pihak ketiga baru yang mengirimkan temuan ke Security Hub CSPM.	12 Juni 2023

Kontrol keamanan yang ada ditambahkan ke Service-Managed Standar: AWS Control Tower	Kontrol CSPM Hub Keamanan yang ada berikut telah ditambahkan ke Service-Managed Standar:. AWS Control Tower • the section called “[Account.1] Informasi kontak keamanan harus disediakan untukAkun AWS” • the section called “[APIGateway.8] Rute API Gateway harus menentukan jenis otorisasi” • the section called “[APIGateway.9] Logging akses harus dikonfigurasi untuk API Gateway V2 Stages” • the section called “[CodeBuild.3] CodeBuild Log S3 harus dienkripsi” • the section called “[EC2.25] Templat peluncuran Amazon EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan” • the section called “[ELB.1] Application Load Balancer harus dikonfigurasi untuk mengarahkan semua permintaan HTTP ke HTTPS” • the section called “[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat”	12 Juni 2023

- the section called “[SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus”
- the section called “[SageMaker.3] Pengguna tidak boleh memiliki akses root ke instance SageMaker notebook”
- the section called “[WAF.10] AWS WAFACL web harus memiliki setidaknya satu aturan atau kelompok aturan”

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia: • the section called “[ACM.2] Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit” • the section called “[AppSync.2]AWS AppSyncharus mengaktifkan logging tingkat lapangan” • the section called “[CloudFront.13] CloudFront distribusi harus menggunakan kontrol akses asal” • the section called “[Elastic Beanstalk.3] Elastic Beanstalk harus mengalirkan log ke CloudWatch” • the section called “[S3.17] Bucket tujuan umum S3 harus dienkripsi saat diam dengan AWS KMS keys” • the section called “[StepFunctions.1] Mesin status Step Functions seharusnya mengaktifkan logging”	6 Juni 2023

Security Hub CSPM tersedia di Asia Pasifik (Melbourne)	Security Hub CSPM sekarang tersedia di Asia Pasifik (Melbourne). Semua fitur CSPM Security Hub sekarang tersedia di Wilayah ini, dengan pengecualian kontrol keamanan tertentu. Untuk informasi selengkapnya, lihat Ketersediaan kontrol menurut Wilayah.	25 Mei 2023
Menemukan sejarah	Security Hub CSPM sekarang dapat melacak riwayat temuan selama 90 hari terakhir.	4 Mei 2023
Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia: • the section called “[EKS.1] Titik akhir cluster EKS tidak boleh diakses publik” • the section called “[ELB.16] Penyeimbang Beban Aplikasi harus dikaitkan dengan AWS WAF ACL web” • the section called “[Redshift.10] Cluster Redshift harus dienkripsi saat istirahat” • the section called “[S3.15] Bucket tujuan umum S3 harus mengaktifkan Object Lock”	29 Maret 2023

Dukungan yang diperluas untuk temuan kontrol konsolidasi	Respon Keamanan Otomatis pada AWS v2.0.0 sekarang mendukung temuan kontrol konsolidasi.	24 Maret 2023
Security Hub CSPM tersedia dalam versi baru Wilayah AWS	Security Hub CSPM sekarang tersedia di Asia Pasifik (Hyderabad), Eropa (Spanyol) , dan Eropa (Zurich). Ada batasan kontrol yang tersedia di Wilayah ini.	21 Maret 2023
Perbarui ke kebijakan terkelola	Security Hub CSPM telah memperbarui izin yang ada dalam kebijakan terkel `AWSSecurityHubServiceRolePolicy` ola.	Maret 17, 2023

Kontrol keamanan baru untuk standar NIST 800-53	Security Hub CSPM telah menambahkan kontrol keamanan berikut, yang berlaku untuk standar NIST 800-53: • the section called “[Account.2]Akun AWSharus menjadi bagian dariAWS Organizationsorganisasi” • the section called “[CloudWatch.15] CloudWatch alarm harus memiliki tindakan tertentu yang dikonfigurasi” • the section called “[CloudWatch.16] CloudWatch grup log harus dipertahankan untuk jangka waktu tertentu” • the section called “[CloudWatch.17] tindakan CloudWatch alarm harus diaktifkan” • the section called “[DynamoDB.4] Tabel DynamoDB harus ada dalam rencana cadangan” • the section called “[EC2.28] Volume EBS harus dicakup oleh rencana cadangan” • EC2.29 - Instans EC2 harus diluncurkan dalam VPC (pensiun) • the section called “[RDS.26] Instans DB RDS harus dilindungi oleh rencana cadangan”	3 Maret 2023

	• the section called “[S3.14] Bucket tujuan umum S3 harus mengaktifkan pembuatan versi” • the section called “[WAF.11] AWS WAFpencatatan ACL web harus diaktifkan”	
Institut Standar dan Teknologi Nasional (NIST) 800-53 Rev. 5	Security Hub CSPM sekarang mendukung standar NIST 800-53 Rev. 5 dengan lebih dari 200 kontrol keamanan yang berlaku.	28 Februari 2023
Tampilan kontrol terkonsolidasi dan temuan kontrol	Dengan rilis tampilan kontrol konsolidasi, halaman Kontrol konsol CSPM Hub Keamanan menampilkan semua kontrol Anda di seluruh standar. Setiap kontrol memiliki ID kontrol yang sama di seluruh standar. Saat Anda mengaktifkan temuan kontrol konsolidasi, Anda menerima satu temuan per pemeriksaan keamanan bahkan ketika kontrol berlaku untuk beberapa standar yang diaktifkan.	23 Februari 2023

Kontrol keamanan baru	Kontrol CSPM Security Hub baru berikut tersedia. Beberapa kontrol memiliki keterbatasan Regional. • the section called “[ElastiCache.1] ElastiCache (Redis OSS) cluster harus mengaktifkan backup otomatis” • the section called “[ElastiCache.2] ElastiCache cluster harus mengaktifkan peningkatan versi minor otomatis” • the section called “[ElastiCache.3] grup ElastiCache replikasi harus mengaktifkan failover otomatis” • the section called “[ElastiCache.4] grup ElastiCache replikasi harus dienkripsi saat istirahat” • the section called “[ElastiCache.5] grup ElastiCache replikasi harus dienkripsi dalam perjalanan” • the section called “[ElastiCache.6] ElastiCache (Redis OSS) grup replikasi dari versi sebelumnya harus mengaktifkan Redis OSS AUTH” • the section called “[ElastiCache.7] ElastiCache cluster	16 Februari 2023

	tidak boleh menggunakan grup subnet default”	
Bidang ASFF baru	Security Hub CSPM telah menambahkan ProductFields.ArchivalReasons:0/Description dan ProductFields.ArchivalReasons:0/ReasonCode ke AWS Security Finding Format (ASFF).	Februari 8, 2023
Bidang ASFF baru	Security Hub CSPM telah menambahkan Compliance.AssociatedStandards dan Compliance.SecurityControlId ke AWS Security Finding Format (ASFF).	31 Januari 2023
Detail kerentanan sekarang tersedia	Anda sekarang dapat melihat detail kerentanan di konsol CSPM Security Hub untuk temuan yang dikirim Amazon Inspector ke Security Hub CSPM.	Januari 14, 2023
Security Hub CSPM tersedia di Timur Tengah (UEA)	Security Hub CSPM sekarang tersedia di Timur Tengah (UEA). Beberapa kontrol memiliki batas Regional.	Januari 12, 2023
Menambahkan integrasi pihak ketiga dengan MetricStream	Security Hub CSPM sekarang mendukung integrasi pihak ketiga dengan MetricStream di semua Wilayah kecuali China dan. AWS GovCloud (US)	11 Januari 2023

Peningkatan batas akun organisasi	Security Hub CSPM sekarang mendukung hingga 11.000 akun anggota untuk setiap akun administrator CSPM Hub Keamanan per Wilayah.	Desember 27, 2022
ElasticBeanstalk.3 digulirkan kembali	Security Hub CSPM memutar kembali kontrol [ElasticBeanstalk.3] Elastic Beanstalk harus melakukan streaming log ke CloudWatch dari standar FSBP di semua Wilayah.	21 Desember 2022
Security Hub CSPM menambahkan kontrol keamanan baru	Kontrol CSPM Security Hub baru tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Beberapa kontrol memiliki keterbatasan Regional.	15 Desember 2022
Panduan tentang fitur yang akan datang	Security Hub CSPM berencana untuk merilis dua fitur baru: tampilan kontrol konsolidasi dan temuan kontrol konsolidasi. Fitur-fitur yang akan datang ini dapat memengaruhi alur kerja yang ada yang bergantung pada bidang dan nilai pencarian kontrol.	Desember 9, 2022
Integrasi Amazon Security Lake sekarang tersedia	Security Lake sekarang terintegrasi dengan Security Hub CSPM dengan menerima temuan Security Hub CSPM.	29 November 2022

Dukungan untuk Service-Managed Standar: AWS Control Tower	Security Hub CSPM mendukung standar keamanan baru yang disebut Service-Managed Standar:. AWS Control Tower AWS Control Tower mengelola standar ini.	28 November 2022
CIS Foundations AWS Benchmark v1.4.0 sekarang tersedia di Wilayah China	Security Hub CSPM sekarang mendukung CIS Foundations AWS Benchmark v1.4.0 di Wilayah China.	18 November 2022
Integrasi Jira Service Management Cloud sekarang tersedia	Jira Service Management Cloud kini menerima temuan Security Hub CSPM di semua Wilayah yang tersedia, kecuali Wilayah China.	17 November 2022
AWS IoT Device Defender integrasi sekarang tersedia	AWS IoT Device Defender sekarang mengirimkan temuan ke Security Hub CSPM di semua Wilayah yang tersedia.	17 November 2022
Dukungan untuk CIS Foundations AWS Benchmark v1.4.0	Security Hub CSPM sekarang menyediakan kontrol keamanan yang mendukung CIS Foundations AWS Benchmark v1.4.0. Standar ini tersedia di semua Wilayah yang tersedia, kecuali Wilayah China.	9 November 2022

Dukungan untuk pengumuman CSPM Security Hub di AWS GovCloud (US)	Anda sekarang dapat berlangganan pengumuman Security Hub CSPM dengan Amazon Simple Notification Service (Amazon SNS) di AWS GovCloud () dan AWS GovCloud (US-EastUS-West) untuk menerima pemberitahuan tentang Security Hub CSPM.	3 Oktober 2022
AWS Security Hub CSPM menambahkan kontrol keamanan baru	Kontrol Security Hub CSPM baru AutoScaling.9 tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Kontrol mungkin memiliki keterbatasan regional.	September 1, 2022
Berlangganan pengumuman Security Hub CSPM	Anda sekarang dapat berlangganan pengumuman Security Hub CSPM dengan Amazon Simple Notification Service (Amazon SNS) untuk menerima pemberitahuan tentang Security Hub CSPM.	Agustus 29, 2022
Ekspansi wilayah untuk agregasi lintas wilayah	Cross-Region agregasi sekarang tersedia untuk temuan, menemukan pembaruan, dan wawasan di seluruh AWS GovCloud (US).	2 Agustus 2022

Integrasi produk pihak ketiga baru	Fortinet - FortiCNP adalah integrasi pihak ketiga yang menerima temuan Security Hub CSPM, dan JFrog adalah integrasi pihak ketiga yang mengirimkan temuan ke Security Hub CSPM.	26 Juli 2022
EC2.27 sudah pensiun	Security Hub CSPM telah dihentikan EC2.27 - Menjalankan Instans EC2 tidak boleh menggunakan pasangan kunci, kontrol sebelumnya dalam standar AWS Foundational Security Best Practices (FSBP).	20 Juli 2022
Lambda.2 tidak lagi mendukung python3.6	Security Hub CSPM tidak lagi mendukung python3.6 sebagai parameter untuk Lambda.2 - Fungsi Lambda harus menggunakan runtime yang didukung, kontrol dalam standar AWS Foundatio nal Security Best Practices (FSBP).	19 Juli 2022
AWS Security Hub CSPM menambahkan kontrol keamanan baru	Kontrol CSPM Security Hub baru tersedia untuk pelanggan yang telah mengaktifkan standar FSBP. Beberapa kontrol memiliki keterbatasan Regional.	Juni 22, 2022

AWS Security Hub CSPM mendukung Wilayah baru	Security Hub CSPM kini tersedia di Asia Pasifik (Jakarta). Beberapa kontrol tidak tersedia di Wilayah ini.	7 Juni 2022
Peningkatan integrasi antara AWS Security Hub CSPM dan AWS Config	Pengguna Security Hub CSPM dapat melihat hasil evaluasi AWS Config aturan sebagai temuan di Security Hub CSPM.	6 Juni 2022
Menambahkan kemampuan untuk memilih keluar dari standar yang diaktifkan secara otomatis	Untuk pengguna yang telah terintegrasi dengan AWS Organizations, fitur ini memungkinkan Anda untuk masuk ke akun administrator CSPM Hub Keamanan dan memilih akun anggota baru di luar standar yang diaktifkan secara otomatis.	April 25, 2022
Agregasi lintas wilayah yang diperluas	Menambahkan agregasi lintas wilayah untuk mengontrol status dan skor keamanan.	20 April 2022
CompanyName dan ProductName sekarang menjadi atribut tingkat atas	Menambahkan atribut tingkat atas baru untuk menetapkan nama perusahaan dan produk yang terkait dengan integrasi kustom	1 April 2022
Menambahkan kontrol baru ke standar AWS Praktik Terbaik Keamanan Dasar	Menambahkan 5 kontrol baru ke standar AWS Praktik Terbaik Keamanan Dasar.	31 Maret 2022
Menambahkan objek detail sumber daya baru ke ASFF	Menambahkan jenis `AwsRdsDbSecurityGroup` sumber daya ke ASFF.	Maret 25, 2022

Menambahkan detail sumber daya tambahan di ASFF	Menambahkan detail tambahan ke`AwsAutoScalingScalingGroup` ,`AwsElbLoadBalancer` ,`AwsRedshiftCluster` , dan`AwsCodeBuildProject` .	Maret 25, 2022
Menambahkan kontrol baru ke standar AWS Praktik Terbaik Keamanan Dasar	Menambahkan 15 kontrol baru ke standar AWS Praktik Terbaik Keamanan Dasar.	16 Maret 2022
Menambahkan kontrol baru ke standar AWS Praktik Terbaik Keamanan Dasar dan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan kontrol baru untuk Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing, dan standar CloudFront Praktik AWS Terbaik Keamanan Dasar. Juga menambahkan dua kontrol baru untuk OpenSearch Layanan ke PCI DSS.	Februari 15, 2022
Menambahkan bidang baru ke ASFF	Ditambahkan bidang baru: Sampel.	26 Januari 2022
Ditambahkan integrasi dengan AWS Health	AWS Health menggunakan pesan peristiwa layanan-ke-layanan untuk mengirim temuan ke Security Hub CSPM.	Januari 19, 2022

Ditambahkan integrasi dengan AWS Trusted Advisor	Trusted Advisor mengirimkan hasil pemeriksaan ke Security Hub CSPM sebagai temuan Security Hub CSPM. Security Hub CSPM mengirimkan hasil pemeriksaan Praktik Terbaik AWS Keamanan Dasarnya ke. Trusted Advisor	18 Januari 2022
Objek detail sumber daya yang diperbarui di ASFF	Ditambahkan `MixedInstancesPolicy` dan `AvailabilityZones` ke`AwsAutoScalingAutoScalingGroup` . Menambahkan `MetadataOptions` ke `AwsAutoScalingLaunchConfiguration` . Menambahkan `BucketVersioningConfiguration` ke `AwsS3Bucket` .	Desember 20, 2021
Output yang diperbarui untuk dokumentasi ASFF	Deskripsi atribut ASFF sebelumnya dalam satu topik. Setiap objek tingkat atas dan setiap objek detail sumber daya sekarang dalam topiknya sendiri. Topik sintaks ASFF berisi tautan ke topik tersebut.	Desember 20, 2021

Menambahkan objek detail sumber daya baru ke ASFF untuk AWS Network Firewall	Untuk AWS Network Firewall, menambahkan objek detail sumber daya berikut:`AwsNetworkFirewallFirewall` ,`AwsNetworkFireFirewallPolicy` , dan`AwsNetworkFirewallRuleGroup` .	Desember 20, 2021
Menambahkan dukungan untuk versi baru Amazon Inspector	Security Hub CSPM terintegrasi dengan versi baru Amazon Inspector serta dengan Amazon Inspector Classic. Amazon Inspector mengirimkan temuan ke Security Hub CSPM.	29 November 2021
Mengubah tingkat keparahan EC2.19	Tingkat keparahan EC2.19 (Grup keamanan tidak boleh mengizinkan akses tidak terbatas ke port dengan risiko tinggi) diubah dari Tinggi ke Kritis.	17 November 2021
Integrasi baru dengan Sonrai Dig	Security Hub CSPM sekarang menawarkan integrasi dengan. Sonrai Dig Sonrai Digmemantau lingkungan cloud untuk mengidentifikasi risiko keamanan. Sonrai Digmengirimkan temuan ke Security Hub CSPM.	12 November 2021

Pemeriksaan yang diperbarui untuk CIS 2.1 dan CloudTrail.1 kontrol	Selain memeriksa bahwa setidaknya satu jalur Multi-wilayah CloudTrail sudah ada, CIS 2.1 dan CloudTrail.1 sekarang juga periksa apakah `ExcludeManagementEventSources` parameter kosong di setidaknya salah satu jalur Multi-region CloudTrail .	9 November 2021
Menambahkan dukungan untuk titik akhir VPC	Security Hub CSPM sekarang terintegrasi dengan AWS PrivateLink dan mendukung titik akhir VPC.	3 November 2021
Menambahkan kontrol ke standar AWS Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Elastic Load Bal ELB.2 ancing (dan ELB.8) dan AWS Systems Manager (SSM.4).	2 November 2021
Menambahkan port untuk memeriksa EC2.19 kontrol	EC2.19 sekarang juga memeriksa bahwa grup keamanan tidak mengizinkan akses masuk tanpa batas ke port berikut: 3000 (Go, Node.js, dan Ruby web development framework), 5000 (kerangka kerja pengembangan web Python), 8088 (port HTTP lama), dan 8888 (port HTTP alternatif)	27 Oktober 2021

Menambahkan integrasi dengan Logz.io Cloud SIEM	Logz.io adalah penyedia Cloud SIEM yang menyediakan korelasi lanjutan dari log dan data peristiwa untuk membantu tim keamanan mendeteksi, menganalisis, dan menanggapi ancaman keamanan secara real time. Logz.io menerima temuan dari Security Hub CSPM.	25 Oktober 2021
Menambahkan dukungan untuk agregasi temuan lintas wilayah	Cross-Region agregasi memungkinkan Anda untuk melihat semua temuan Anda tanpa harus mengubah Wilayah. Akun administrator memilih Wilayah agregasi dan Wilayah tertaut. Temuan untuk akun administrator dan akun anggotanya dikumpulkan dari Wilayah yang ditautkan ke Wilayah agregasi.	20 Oktober 2021
Objek detail sumber daya yang diperbarui di ASFF	Menambahkan detail sertifikat penampil ke`AwsCloudFrontDistribution`. Menambahkan detail tambahan ke`AwsCodeBuildProject`. Menambahkan atribut penyeimbang beban ke`AwsElbV2LoadBalancer`. Menambahkan pengenal akun pemilik bucket S3 ke`AwsS3Bucket`.	Oktober 8, 2021

Menambahkan objek detail sumber daya baru ke ASFF	Menambahkan objek detail sumber daya baru berikut ke ASFF:`AwsEc2VpcEndpointService` ,,`AwsEcrRepository` ,`AwsEksCluster` ,`AwsOpenSearchServiceDomain` ,`AwsWafRateBasedRule` , `AwsWafRegionalRateBasedRule` `AwsXrayEncryptionConfig`	Oktober 8, 2021
Menghapus runtime yang tidak digunakan lagi dari kontrol Lambda.2	Dalam standar AWS Praktik Terbaik Keamanan Dasar, `dotnetcore2.1` runtime yang dihapus dari [Lambda.2] Fungsi Lambda harus menggunakan runtime yang didukung.	Oktober 6, 2021
Nama baru untuk integrasi Check Point	Integrasi dengan Check Point Dome9 Arc sekarang menjadi Check Point Posture Management CloudGuard. Integrasi ARN tidak berubah.	1 Oktober 2021
Menghapus integrasi dengan Alcide	Integrasi dengan Alcide KAudit dihentikan.	30 September 2021
Mengubah tingkat keparahan EC2.19	Tingkat keparahan [EC2.19] Grup keamanan tidak boleh mengizinkan akses tak terbatas ke port dengan risiko tinggi diubah dari Sedang ke Tinggi.	30 September 2021

Integrasi dengan AWS Organizations sekarang didukung di Wilayah China	Integrasi Security Hub CSPM dengan Organisasi sekarang didukung di China (Beijing) dan China (Ningxia).	September 20, 2021
A AWS Config turan baru untuk PCI.S3.6 kontrol S3.1 dan	K S3.1 edu PCI.S3.6 anya dan verifikasi bahwa setelan Amazon S3 Block Public Access diaktifkan. A AWS Config turan untuk kontrol ini diubah dari `s3-account-level-public-access-blocks` menjadi`s3-account-level-public-access-blocks-periodic` .	14 September 2021
Menghapus runtime yang tidak digunakan lagi dari kontrol Lambda.2	Dalam standar AWS Praktik Terbaik Keamanan Dasar, fungsi `nodejs10.x` dan `ruby2.5` runtime yang dihapus dari [Lambda.2] Lambda harus menggunakan runtime yang didukung.	13 September 2021
Mengubah tingkat keparahan kontrol CIS 2.2	Dalam standar CIS Foun AWS dations Benchmark, tingkat keparahan untuk 2.2. — Pastikan validasi file CloudTrai l log diaktifkan diubah dari Rendah ke Sedang.	13 September 2021

Diperbarui ECS.1, Lambda.2, dan SSM.1 dalam standar AWS Praktik Terbaik Keamanan Dasar	Dalam standar AWS Praktik Terbaik Keamanan Dasar, ECS.1 sekarang memiliki `SkipInactiveTaskDefinitions` parameter yang disetel ke`true`. Ini memastikan bahwa kontrol hanya memeriksa definisi tugas aktif. Untuk Lambda.2, menambahkan Python 3.9 ke daftar runtime. SSM.1 sekarang memeriksa instans yang dihentikan dan berjalan.	7 September 2021
PCI.Lambda.2 kontrol sekarang mengecualikan sumber daya Lambda @Edge	Dalam standar Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS), PCI.Lambda.2 kontrol sekarang mengecualikan sumber daya Lambda @Edge.	7 September 2021
Menambahkan integrasi dengan HackerOne Vulnerability Intelligence	Security Hub CSPM sekarang menawarkan integrasi dengan. HackerOne Vulnerability Intelligence Integrasi mengirimkan temuan ke Security Hub CSPM.	7 September 2021

Objek detail sumber daya yang diperbarui di ASFF	Untuk `AwsKmsKey`, ditambahkan `KeyRotationStatus`. Untuk `AwsS3Bucket`, ditambahkan `AccessControlList`, `BucketLoggingConfiguration`, `BucketNotificationConfiguration`, dan `BucketWebsiteConfiguration`.	2 September 2021
Menambahkan objek detail sumber daya baru ke ASFF	Menambahkan objek detail sumber daya baru berikut ke ASFF: `AwsAutoScalingLaunchConfiguration`, `AwsEc2VpnConnection`, dan `AwsEcrContainerImage`.	2 September 2021
Menambahkan detail ke `Vulnerabilities` objek di ASFF	Di dalam `Cvss`, menambahkan `Adjustments` dan `Source`. Di `VulnerablePackages`, menambahkan jalur file dan manajer paket.	2 September 2021
System Manager Explorer dan OpsCenter integrasi sekarang didukung di Wilayah China	Integrasi Security Hub CSPM dengan SSM Explorer dan sekarang OpsCenter didukung di China (Beijing) dan China (Ningxia).	31 Agustus 2021

Menghentikan kontrol Lambda.4	Security Hub CSPM menghentikan kontrol [Lambda.4] Fungsi lambda harus memiliki antrian huruf mati yang dikonfigurasi. Ketika kontrol dihentikan, kontrol tidak lagi ditampilk an di konsol, dan Security Hub CSPM tidak melakukan pemeriksaan terhadapnya.	31 Agustus 2021
Menghentikan kontrol PCI.EC2.3	Security Hub CSPM menghentikan kontrol [PCI.EC2.3] Grup keamanan EC2 yang tidak digunakan harus dihapus. Ketika kontrol dihentikan, kontrol tidak lagi ditampilkan di konsol, dan Security Hub CSPM tidak melakukan pemeriksaan terhadapnya.	Agustus 27, 2021
Mengubah cara Security Hub CSPM mengirimkan temuan ke tindakan kustom	Saat Anda mengirim temuan ke tindakan kustom, Security Hub CSPM sekarang mengirimkan setiap temuan dalam acara terpisah Security Hub Findings - Custom Action.	Agustus 20, 2021

Menambahkan kode alasan status kepatuhan baru untuk runtime Lambda kustom	Menambahkan kode alasan status `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` kepatuhan baru. Kode alasan ini menunjukkan bahwa Security Hub CSPM tidak dapat melakukan pemeriksaan terhadap runtime Lambda kustom.	Agustus 20, 2021
AWS Firewall Manager integrasi sekarang didukung di Wilayah China	Integrasi Security Hub CSPM dengan Firewall Manager sekarang didukung di China (Beijing) dan China (Ningxia).	19 Agustus 2021
Integrasi baru dengan dan Caveonix CloudForcepoint Cloud Security Gateway	Security Hub CSPM sekarang menawarkan integrasi dengan dan. Caveonix Cloud Forcepoint Cloud Security Gateway Kedua integrasi mengirimkan temuan ke Security Hub CSPM.	Agustus 10, 2021

Menambahkan `Region` atribut baru `CompanyName` `ProductName` ,, dan ke ASFF	Dit `CompanyName` ambahkan`ProductName` ,, dan `Region` bidang ke tingkat atas ASFF. Bidang-bidang ini diisi secara otomatis dan, kecuali untuk integrasi produk khusus, tidak dapat diperbarui menggunakan `BatchImportFindings` atau`BatchUpdateFindings` . Di konsol, menemukan filter menggunakan bidang baru ini. Di API, `ProductName` filter `CompanyName` dan menggunakan atribut yang ada di bawah`ProductFields` .	23 Juli 2021
Menambahkan dan memperbarui objek detail sumber daya di ASFF	Menambahkan jenis `AwsRdsEventSubscription` sumber daya baru dan detail sumber daya. Menambahkan detail sumber daya untuk jenis `AwsEcsService` sumber daya. Menambahkan atribut ke objek detail `AwsElasticsearchDomain` sumber daya.	23 Juli 2021

Menambahkan kontrol ke standar AWS Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5 melalui ES.8), Amazon RDS (RDS.16 melalui RDS.23), Amazon Redshift (), dan Amazon SQS (Redshift.4). SQS.1	20 Juli 2021
Memindahkan izin dalam kebijakan yang dikelola peran terkait layanan	Memindahkan `config:PutEvaluations` izin dalam kebijakan terkelola`AWSSecurityHubServiceRolePolicy` , sehingga diterapkan ke semua sumber daya.	14 Juli 2021
Menambahkan kontrol ke standar AWS Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.4), Amazon CloudFront (CloudFront.5 dan CloudFront.6), Amazon EC2 (EC2.17 dan EC2.18), Amazon ECS (ECS.1), Amazon OpenSearch Service (ES.4), AWS Identity and Access Management (IAM.21), Amazon RDS (RDS.15), dan Amazon S3 (). S3.8	8 Juli 2021

Menambahkan kode alasan status kepatuhan baru untuk temuan kontrol	`INTERNAL_SERVICE_ERROR` menunjukkan bahwa kesalahan yang tidak diketahui terjadi. `SNS_TOPIC_CROSS_ACCOUNT` menunjukkan bahwa topik SNS dimiliki oleh akun yang berbeda. `SNS_TOPIC_INVALID` menunjukkan bahwa topik SNS terkait tidak valid.	6 Juli 2021
Menambahkan integrasi dengan Amazon Q Developer di aplikasi obrolan	Menambahkan integrasi dengan Amazon Q Developer dalam aplikasi obrolan. Security Hub CSPM mengirimkan temuan ke Amazon Q Developer dalam aplikasi obrolan.	30 Juni 2021
Menambahkan izin baru ke kebijakan yang dikelola peran terkait layanan	Menambahkan izin baru ke kebijakan terkelola `AWSSecurityHubServiceRolePolicy` untuk mengizinkan peran terkait layanan mengirimkan hasil evaluasi ke. AWS Config	29 Juni 2021

Objek detail sumber daya baru dan diperbarui di ASFF	Menambahkan objek detail sumber daya baru untuk cluster ECS dan definisi tugas ECS. Memperbarui objek instance EC2 untuk mencantumkan antarmuka jaringan terkait. Menambahkan ID sertifikat klien untuk tahap API Gateway V2. Menambahkan konfigurasi siklus hidup untuk bucket S3.	24 Juni 2021
Memperbarui perhitungan status kontrol agregat dan skor keamanan standar	Security Hub CSPM sekarang menghitung status kontrol keseluruhan dan skor keamanan standar setiap 24 jam. Untuk akun administrator, skor sekarang mencerminkan apakah setiap kontrol diaktifkan atau dinonaktifkan untuk setiap akun.	23 Juni 2021
Informasi terbaru tentang penanganan CSPM Security Hub terhadap akun yang ditangguhkan	Menambahkan informasi tentang cara Security Hub CSPM menangani akun yang ditangguhkan. AWS	23 Juni 2021
Menambahkan tab untuk menampilkan kontrol yang diaktifkan dan dinonaktifkan untuk akun administrator individu	Untuk akun administrator, tab utama pada halaman detail standar berisi informasi agregat di seluruh akun. Tab baru Diaktifkan untuk akun ini dan Dinonaktifkan untuk akun ini mencantumkan akun yang diaktifkan atau dinonaktifkan untuk akun administrator individu.	23 Juni 2021

Dit `java8.al2` ambahkan ke parameter untuk `Lambda.2`	Dalam standar AWS Praktik Terbaik Keamanan Dasar, ditambahkan `java8.al2` ke runtime yang didukung untuk kontrol. `Lambda.2`	8 Juni 2021
Integrasi baru dengan MicroFocus ArcSight dan NETSCOUT Cyber Investigator	Menambahkan integrasi dengan MicroFocus ArcSight dan NETSCOUT Cyber Investigator. MicroFocus ArcSight menerima temuan dari Security Hub CSPM. NETSCOUT Cyber Investigator mengirimkan temuan ke Security Hub CSPM.	7 Juni 2021
Menambahkan detail untuk `AWSSecurityHubServiceRolePolicy`	Memperbarui bagian kebijakan terkelola untuk menambahkan detail kebijakan terkelola yang ada`AWSSecurityHubServiceRolePolicy`, yang digunakan oleh peran terkait layanan CSPM Hub Keamanan.	4 Juni 2021
Integrasi baru dengan Jira Service Management	Konektor Manajemen AWS Layanan untuk Jira mengirimkan temuan ke Jira dan menggunakannya untuk membuat masalah Jira. Ketika masalah Jira diperbarui, temuan terkait di Security Hub CSPM juga diperbarui.	26 Mei 2021

Memperbarui daftar kontrol yang didukung untuk Wilayah Asia Pasifik (Osaka)	Memperbarui standar AWS CIS Foundation dan Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) untuk menunjukkan kontrol yang tidak didukung di Asia Pasifik (Osaka).	21 Mei 2021
Integrasi baru dengan Sysdig Secure untuk cloud	Menambahkan integrasi dengan Sysdig Secure untuk cloud. Integrasi mengirimk an temuan ke Security Hub CSPM.	14 Mei 2021
Menambahkan kontrol ke standar AWS Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.2 dan APIGateway.3), AWS CloudTrail (CloudTrail.4 dan CloudTrail.5), Amazon EC2 (EC2.15 dan EC2.16), AWS Elastic Beanstalk (Elastic Beanstalk.1 dan ElasticBe anstalk.2), AWS Lambda (Lambda.4), Amazon RDS (RDS.12— RDS.14), Amazon Redshift (Redshift.7), (dan), SecretsManager.3 dan AWS Secrets Manager (SecretsMa nager.4). AWS WAF WAF.1	10 Mei 2021
Pembaruan untuk GuardDuty dan kontrol Amazon RDS	Mengubah tingkat keparahan `GuardDuty.1` dan `PCI.GuardDuty.1` dari Sedang ke Tinggi. Menambahkan `databaseE ngines` parameter ke`RDS.8`.	4 Mei 2021

Menambahkan detail sumber daya baru ke ASFF	Di`Resources.Details` , menambahkan objek detail sumber daya baru untuk ACL jaringan Amazon EC2, subnet Amazon EC2, dan lingkungan. AWS Elastic Beanstalk	3 Mei 2021
Menambahkan bidang konsol untuk memberikan nilai filter untuk EventBridge aturan Amazon	Pola filter baru yang telah ditentukan sebelumnya untuk EventBridge aturan CSPM Security Hub menyediak an bidang konsol yang dapat Anda gunakan untuk menentukan nilai filter.	30 April 2021
Menambahkan integrasi dengan AWS Systems Manager Explorer dan OpsCenter	Security Hub CSPM sekarang mendukung integrasi dengan Systems Manager Explorer dan. OpsCenter Integrasi menerima temuan dari Security Hub CSPM dan memperbarui temuan tersebut di Security Hub CSPM.	26 April 2021
Tipe baru untuk integrasi produk	Jenis integrasi baru,`UPDATE_FINDINGS_IN _SECURITY_HUB` , menunjukkan bahwa integrasi produk memperbarui temuan yang diterimanya dari Security Hub CSPM.	22 April 2021
Mengubah “akun master” menjadi “akun administrator”	Istilah "akun utama" diubah menjadi "akun administrator." Istilah ini juga diubah di konsol CSPM Security Hub dan API.	22 April 2021

Diperbarui APIGateway.1 untuk mengganti HTTP dengan Websocket	Memperbarui judul, deskripsi , dan remediasi untuk APIGateway.1. Kontrol sekarang memeriksa logging eksekusi API Websocket alih-alih logging eksekusi API HTTP.	9 April 2021
GuardDuty Integrasi Amazon sekarang didukung di Beijing dan Ningxia	Integrasi Security Hub CSPM sekarang GuardDuty didukung di Wilayah China (Beijing) dan China (Ningxia).	5 April 2021
Ditambahkan `nodejs14.x` ke runtime yang didukung untuk kontrol Lambda.2	Lambda.2 Kontrol dalam standar Praktik Terbaik Keamanan Dasar sekarang mendukung `nodejs14.x` runtime.	30 Maret 2021
Security Hub CSPM diluncurkan di Asia Pasifik (Osaka)	Security Hub CSPM sekarang tersedia di Wilayah Asia Pasifik (Osaka).	29 Maret 2021
Menambahkan bidang penyedia pencarian untuk menemukan detail	Pada panel rincian temuan, bagian Bidang Penye dia Pencari yang baru berisi nilai penyedia temuan untuk kepercayaan, kekritisa n, temuan terkait, tingkat keparahan, dan jenis.	24 Maret 2021
Ditambahkan opsi untuk menerima temuan sensitif dari Amazon Macie	Integrasi dengan Macie sekarang dapat dikonfigu rasi untuk mengirim temuan sensitif ke Security Hub CSPM.	23 Maret 2021

Transisi ke AWS Organizations untuk manajemen akun	Untuk pelanggan yang memiliki akun administrator yang sudah ada dengan akun anggota, menambahkan informasi baru tentang cara mengubah dari mengelola akun dengan undangan ke mengelola akun menggunakan Organisasi.	22 Maret 2021
Objek baru di ASFF untuk informasi tentang konfigurasi Blok Akses Publik Amazon S3	Di`Resources` , jenis `AwsS3AccountPublicAccessBlock` sumber daya dan objek detail baru menyediakan informasi tentang konfigurasi Blok Akses Publik Amazon S3 untuk akun. Dalam objek detail `AwsS3Bucket` sumber daya, `PublicAccessBlockConfiguration` objek menyediakan konfigurasi Blok Akses Publik untuk bucket S3.	18 Maret 2021

Objek baru di ASFF untuk memungkinkan penyedia pencarian memperbarui bidang tertentu	Ob `FindingProviderFields` jek baru di ASFF digunakan `BatchImportFindings` untuk memberikan nilai untuk`Confidence` ,,`Criticality` , `RelatedFindings` `Severity`, dan`Types`. Bidang asli hanya boleh diperbarui menggunakan`BatchUpdateFindings` .	18 Maret 2021
Ob `DataClassification` jek baru untuk sumber daya di ASFF	Ob `Resources.DataClassification` jek baru di ASFF digunakan untuk memberikan informasi tentang data sensitif yang terdeteksi pada sumber daya.	18 Maret 2021
Nilai `CONFIG_RETURNS_NOT_APPLICABLE` tambah ke kode status kepatuhan yang tersedia	Untuk status `NOT_AVAILABLE` kepatuhan, hapus kode alasan `RESOURCE_NO_LONGER_EXISTS` dan tambahkan kode alasan`CONFIG_RETURNS_NOT_APPLICABLE` .	16 Maret 2021

Kebijakan terkelola baru untuk integrasi dengan AWS Organizations	Kebijakan terkelola baru`AWSSecurityHubOrganizationsAccess` ,, menyediakan izin Organisasi yang diperlukan oleh akun manajemen organisasi dan akun administrator CSPM Hub Keamanan yang didelegasikan.	15 Maret 2021
Kebijakan terkelola dan informasi peran terkait layanan dipindahkan ke bagian Keamanan	Informasi tentang kebijakan yang dikelola direvisi dan diperluas. Baik informasi kebijakan terkelola maupun informasi tentang peran terkait layanan telah dipindahkan ke bagian Keamanan.	15 Maret 2021
Tingkat keparahan yang direvisi untuk kontrol CIS 1.1 dan CIS 3.1 — CIS 3.14	Tingkat keparahan kontrol CIS 1.1 dan CIS 3.1 — CIS 3.14 diubah menjadi Rendah.	3 Maret 2021
Menghapus RDS.11 kontrol	Menghapus RDS.11 kontrol dari standar Praktik Terbaik Keamanan Dasar.	3 Maret 2021
Integrasi yang diperbarui untuk Turbot	Integrasi Turbot diperbarui untuk mengirim dan menerima temuan.	26 Februari 2021

Menambahkan kontrol ke standar Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 dan EC2.10), Amazon Elastic File System (EFS.2), Amazon OpenSearch Service (ES.2 dan ES.3), Elastic Load Balancing (ELB.6), dan AWS Key Management Service (AWS KMS) (KMS.3).	11 Februari 2021
Menambahkan `ProductArn` filter opsional ke `DescribeProducts` API	Oper `DescribeProducts` asi API sekarang menyertakan `ProductArn` parameter opsional. `ProductArn` Parameter digunakan untuk mengidentifikasi integrasi produk tertentu untuk mengembalikan detailnya.	3 Februari 2021
Integrasi baru dengan Antivirus untuk Amazon S3 dari Cloud Storage Security	Integrasi dengan Antivirus untuk Amazon S3 mengirimkan hasil pemindaian virus ke Security Hub CSPM sebagai temuan.	27 Januari 2021
Memperbarui proses perhitungan skor keamanan untuk akun administrator	Untuk akun administrator, Security Hub CSPM menggunakan proses terpisah untuk menghitung skor keamanan. Proses baru memastikan bahwa skor mencakup kontrol yang diaktifkan untuk akun anggota tetapi dinonaktifkan untuk akun administrator.	21 Januari 2021

Bidang dan objek baru di ASFF	Menambahkan `Action` objek baru untuk melacak tindakan yang terjadi terhadap sumber daya. Menambahkan bidang ke `AwsEc2NetworkInterface` objek untuk melacak nama DNS dan alamat IP. Menambahkan `AwsSsmPatchCompliance` objek baru ke detail sumber daya.	21 Januari 2021
Menambahkan kontrol ke standar Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk Amazon CloudFront (CloudFront.1 melalui CloudFront.4), Amazon DynamoDB (DynamoDB.1 melalui DynamoDB.3), Elastic Load Balancing (ELB.3 melalui ELB.5), Amazon RDS (RDS.9melalui RDS.11), Amazon Redshift (Redshift.1 melalui Redshift.3 dan Redshift.6), dan Amazon SNS (). SNS.1	15 Januari 2021

Status alur kerja diatur ulang berdasarkan status catatan atau status kepatuhan	Security Hub CSPM secara otomatis mengatur ulang status alur kerja dari `NOTIFIED` atau `RESOLVED` ke `NEW` jika temuan yang diarsipkan dibuat aktif, atau jika status kepatuhan temuan berubah dari salah satu `PASSEDFAILED`,, `WARNING` atau. `NOT_AVAILABLE` Perubahan ini menunjukkan bahwa penyelidikan tambahan diperlukan.	7 Januari 2021
Menambahkan `ProductFields` informasi untuk temuan berbasis kontrol	Untuk temuan yang dihasilkan dari kontrol, ditambahkan informasi tentang konten `ProductFields` objek dalam Format Penemuan Keamanan AWS (ASFF).	29 Desember 2020
Pembaruan untuk wawasan terkelola	Mengubah judul wawasan 5. Menambahkan wawasan baru, 32, yang memeriksa pengguna IAM dengan aktivitas mencurigakan.	22 Desember 2020
Pembaruan IAM.7 dan Lambda.1 kontrol	Dalam standar AWS Praktik Terbaik Keamanan Dasar, memperbarui parameter untuk IAM.7. Memperbarui judul dan deskripsi Lambda.1.	22 Desember 2020

Integrasi yang diperluas dengan ServiceNow ITSM	Integrasi ServiceNow ITSM memungkinkan pengguna untuk secara otomatis membuat insiden atau masalah ketika temuan CSPM Security Hub diterima. Pembaruan untuk insiden atau masalah ini mengakibatkan pembaruan pada temuan di Security Hub CSPM.	11 Desember 2020
Integrasi baru dengan AWS Audit Manager	Security Hub CSPM sekarang menawarkan integrasi dengan AWS Audit Manager. Integrasi ini memungkinkan Audit Manager menerima temuan berbasis kontrol dari Security Hub CSPM.	8 Desember 2020
Integrasi baru dengan Aqua Security Kube-bench	Security Hub CSPM menambahkan integrasi dengan Aqua Security. Kube-bench Integrasi mengirimk an temuan ke Security Hub CSPM.	24 November 2020
Cloud Custodian sekarang tersedia di Wilayah China	Integrasi dengan Cloud Custodian sekarang tersedia di China (Beijing) dan China (Ningxia) Wilayah.	24 November 2020

BatchImportFindings sekarang dapat digunakan untuk memperbarui bidang tambahan	Sebelumnya, Anda tidak dapat menggunakan BatchImportFindings untuk memperbarui Types bidang Confidence Criticality ,RelatedFindings ,Severity,, dan. Sekarang, jika bidang ini belum diperbarui olehBatchUpdateFindings , mereka dapat diperbarui olehBatchImportFindings . Setelah diperbarui olehBatchUpdateFindings , mereka tidak dapat diperbarui olehBatchImportFindings .	24 November 2020
Security Hub CSPM sekarang terintegrasi dengan AWS Organizations	Pelanggan sekarang dapat mengelola akun anggota menggunakan konfigurasi akun Organisasi mereka. Akun manajemen organisasi menunjuk akun administrator CSPM Hub Keamanan, yang menentukan akun organisasi mana yang akan diaktifkan di Security Hub CSPM. Proses undangan manual masih dapat digunakan untuk akun yang bukan bagian dari organisasi.	23 November 2020
Menghapus format daftar temuan terpisah untuk kontrol volume tinggi	Daftar temuan untuk kontrol tidak lagi menggunakan format halaman Temuan ketika ada sejumlah besar temuan.	19 November 2020

Integrasi pihak ketiga yang baru dan diperbarui	Security Hub CSPM sekarang mendukung integrasi dengan cloudtamer.io, 3CoreSec, Prowler, dan Kubernete s Security. StackRox IBM QRadar tidak lagi mengirimkan temuan. Itu hanya menerima temuan.	30 Oktober 2020
Ditambahkan opsi untuk mengunduh daftar temuan dari halaman detail kontrol.	Pada halaman detail kontrol, opsi Unduh baru memungkin kan Anda mengunduh daftar pencarian ke file.csv. Daftar yang diunduh menghorma ti filter apa pun yang ada dalam daftar. Jika Anda memilih temuan tertentu, maka daftar yang diunduh hanya menyertakan temuan tersebut.	26 Oktober 2020
Ditambahkan opsi untuk mengunduh daftar kontrol dari halaman detail standar.	Pada halaman detail standar, opsi Unduh baru memungkin kan Anda mengunduh daftar kontrol ke file.csv. Daftar yang diunduh menghorma ti filter apa pun yang ada dalam daftar. Jika Anda memilih kontrol tertentu, maka daftar yang diunduh hanya menyertakan kontrol itu.	26 Oktober 2020

Integrasi mitra baru dan terbaru	Security Hub CSPM sekarang terintegrasi dengan. ThreatModeler Memperbar ui integrasi mitra berikut untuk mencerminkan nama produk baru mereka. Twistlock Enterprise Edition sekarang menjadi Palo Alto Networks - Prisma Cloud Compute. Juga dari Palo Alto Networks, Demisto sekarang Cortex XSOAR dan Redlock sekarang menjadi Prisma Cloud Enterprise.	23 Oktober 2020
Security Hub CSPM diluncurkan di China (Beijing) dan China (Ningxia)	Security Hub CSPM sekarang tersedia di China (Beijing) dan China (Ningxia) Wilayah.	21 Oktober 2020
Format yang direvisi untuk atribut ASFF dan integrasi pihak ketiga	Daftar atribut ASFF dan integrasi mitra sekarang menggunakan format berbasis daftar, bukan tabel. Sintaksis ASFF, atribut, dan taksonomi tipe sekarang berada dalam topik terpisah.	15 Oktober 2020
Halaman detail standar yang didesain ulang	Halaman detail standar untuk standar yang diaktifkan sekarang menampilkan daftar kontrol dengan tab. Tab memfilter daftar kontrol berdasarkan status kontrol.	7 Oktober 2020
Meng CloudWatch ganti acara dengan EventBridge	Mengganti referensi ke Amazon CloudWatch Events dengan Amazon EventBridge.	1 Oktober 2020

Integrasi baru dengan Blue Hexagon untuk AWS, Alcide KAudit, dan Palo Alto Networks. VM-Series	Security Hub CSPM sekarang terintegrasi dengan Blue Hexagon untuk AWS, Alcide KAudit, dan Palo Alto Networks. VM-Series Blue Hexagon untuk AWS dan KAudit mengirim temuan ke Security Hub CSPM. VM-Series menerima temuan dari Security Hub CSPM.	30 September 2020
Objek detail sumber daya baru dan diperbarui di ASFF	Menambahkan `Resources.Details` objek baru untuk `AwsApiGatewayRestApi` `AwsApiGatewayStage` ,,`AwsApiGatewayV2Api` ,`AwsApiGatewayV2Stage` ,`AwsCertificateManagerCertificate` ,`AwsElbLoadBalancer` ,`AwsIamGroup` , dan`AwsRedshiftCluster` . Menambahkan detail ke`AwsCloudFrontDistribution` , `AwsIamRole` dan `AwsIamAccessKey` objek.	30 September 2020
A `ResourceRole` tribut baru untuk sumber daya di ASFF untuk melacak apakah sumber daya adalah aktor atau target.	A `ResourceRole` tribut untuk sumber daya menunjukkan apakah sumber daya adalah target aktivitas penemuan atau pelaku aktivitas penemuan. Nilai yang valid adalah `ACTOR` dan `TARGET`.	30 September 2020

Menambahkan AWS Systems Manager Patch Manager ke integrasi AWS layanan yang tersedia	AWS Systems Manager Patch Manager sekarang terintegrasi dengan Security Hub CSPM. Patch Manager mengirimk an temuan ke Security Hub CSPM ketika instans dalam armada pelanggan tidak sesuai dengan standar kepatuhan patch mereka.	22 September 2020
Menambahkan kontrol baru ke standar AWS Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru untuk layanan berikut: Amazon EC2 (EC2.7 dan EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (RDS.4 melalui RDS.8), Amazon S3 (), dan (dan S3.6 AWS Secrets Manager). SecretsManager.1 SecretsManager.2	15 September 2020
Kunci konteks baru untuk kebijakan IAM untuk mengontrol akses ke bidang `BatchUpdateFindings`	Kebijakan IAM sekarang dapat dikonfigurasi untuk membatasi akses ke bidang dan nilai bidang saat menggunak an`BatchUpdateFinding s` .	10 September 2020
Akses yang diperluas `BatchUpdateFindings` untuk akun anggota	Secara default, akun anggota sekarang memiliki akses yang sama dengan `BatchUpda teFindings` akun administrator.	10 September 2020

Kontrol baru untuk AWS KMS Standar Praktik Terbaik Keamanan Dasar	Menambahkan dua kontrol baru (KMS.1 dan KMS.2) ke Standar Praktik Terbaik Keamanan Dasar. Kontrol baru memeriksa apakah kebijakan IAM membatasi akses ke tindakan AWS KMS dekripsi.	9 September 2020
Dihapus temuan tingkat akun untuk kontrol	Security Hub CSPM tidak lagi menghasilkan temuan tingkat akun untuk kontrol. Hanya temuan tingkat sumber daya yang dihasilkan.	1 September 2020
Ob PatchSummary jek baru di ASFF	Menambahkan `PatchSummary` objek ke ASFF. Ob `PatchSummary` jek memberikan informasi tentang kepatuhan patch sumber daya relatif terhadap standar kepatuhan yang dipilih.	1 September 2020
Halaman detail kontrol yang didesain ulang	Halaman detail untuk kontrol didesain ulang. Daftar pencarian kontrol menyediakan tab untuk memungkinkan Anda memfilter daftar dengan cepat berdasarkan status kepatuhan. Anda juga dapat dengan cepat melihat temuan yang ditekan. Setiap entri menyediakan akses ke detail tambahan tentang sumber daya pencarian, AWS Config aturan, dan catatan pencarian.	28 Agustus 2020

Opsi filter baru untuk temuan	Untuk menemukan filter, Anda dapat menggunakan filter is not untuk menemukan temuan yang nilai bidangnya tidak sama dengan nilai filter. Anda dapat menggunakan does not start with untuk menemukan temuan yang nilai bidangnya tidak dimulai dengan nilai filter yang ditentukan.	28 Agustus 2020
Objek detail sumber daya baru di ASFF	Menambahkan `Resources .Details` objek baru untuk jenis sumber daya berikut: `AwsDynamo DbTable AwsEc2Eip ,AwsIamPol icy ,AwsIamUse r ,AwsRdsDbC luster ,AwsRdsDbC lusterSna pshot ,AwsRdsDbS napshot , AwsSecret sManagerSecret`	18 Agustus 2020
Integrasi baru dengan RSA Archer	Security Hub CSPM sekarang terintegrasi dengan RSA Archer. RSA Archer menerima temuan dari Security Hub CSPM.	18 Agustus 2020
Bidang Deskripsi Baru untuk AwsKmsKey	Menambahkan `Descripti on` bidang ke `AwsKmsKey` objek di bawah`Resources .Details` .	18 Agustus 2020

Bidang ditambahkan ke AwsRdsDbInstance	Menambahkan beberapa atribut ke `AwsRdsDbInstance` objek di bawah `Resources.Details` .	18 Agustus 2020
Memperbarui bagaimana Security Hub CSPM menentukan status keseluruhan kontrol	Untuk kontrol yang tidak memiliki temuan, statusnya adalah Tidak ada data, bukan Tidak Diketahui. Status kontrol mencakup temuan tingkat akun dan tingkat sumber daya. Status kontrol tidak menggunakan status alur kerja temuan, kecuali untuk mengabaikan temuan yang ditekan.	13 Agustus 2020
Memperbarui cara Security Hub CSPM menghitung skor keamanan untuk standar	Saat menghitung skor keamanan untuk standar, Security Hub CSPM sekarang mengabaikan kontrol dengan status Tidak Ada Data. Skor keamanan adalah proporsi kontrol yang dilewati ke kontrol yang diaktifkan, tidak termasuk kontrol tanpa data.	13 Agustus 2020
Opsi baru untuk secara otomatis mengaktifkan kontrol baru dalam standar yang diaktifkan	Menambahkan opsi Peng aturan untuk secara otomatis mengaktifkan kontrol baru dalam standar yang diaktifkan. Anda juga dapat menggunakan operasi `UpdateSecurityHubConfiguration` API untuk mengkonfigurasi opsi ini.	31 Juli 2020

Kontrol baru untuk standar Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan kontrol baru ke standar PCI DSS. Pengidentifikasi kontrol baru adalah PCI.DMS.1,, PCI.EC2.5, PCI.EC2.6 PCI.ELBV2.1, PCI.GuardDuty.1, PCI.IAM.7, PCI.IAM.8, PCI.S3.5, PCI.S3.6, PCI.SageMaker.1, PCI.SSM.2, dan PCI.SSM.3.	29 Juli 2020
Kontrol baru dan diperbarui untuk standar Praktik Terbaik Keamanan Dasar	Menambahkan kontrol baru ke standar Praktik Terbaik Keamanan Dasar. Pengidentifikasi kontrol baru adalah AutoScaling.1, DMS.1, EC2.4, EC2.6, S3.5, dan SSM.3. Memperbarui judul ACM.1 dan mengubah nilai `daysToExpiration` parameter menjadi 30.	29 Juli 2020
Ob `Vulnerabilities` jek baru di ASFF	Menambahkan `Vulnerabilities` objek, yang memberikan informasi tentang kerentanan yang terkait dengan temuan.	1 Juli 2020
Ob `Resource.Details` jek baru di ASFF untuk grup Penskalaan Otomatis, volume EC2, dan VPC EC2	Menambahkan`AwsAutoScalingAutoScalingGroup` ,`AWSEc2Volume` , dan `AwsEc2Vpc` objek ke`Resource.Details` .	1 Juli 2020
Ob `NetworkPath` jek baru di ASFF	Menambahkan `NetworkPath` objek, yang memberikan informasi tentang jalur jaringan yang terkait dengan temuan.	1 Juli 2020

Secara otomatis menyelesaikan temuan `Compliance.Status` ketika `PASSED`	Untuk temuan dari kontrol, jika `Compliance.Status` ada`PASSED`, maka Security Hub CSPM secara otomatis disetel ke. `Workflow.Status` `RESOLVED`	24 Juni 2020
AWS Command Line Interface contoh-contoh	Ditambahkan AWS CLI sintaks dan contoh untuk beberapa tugas Security Hub CSPM. Termasuk mengaktifkan Security Hub CSPM, mengelola wawasan, mengelola standar dan kontrol, mengelola integrasi produk, dan menonaktifkan Security Hub CSPM.	24 Juni 2020
A `Severity.Original` tribut baru di ASFF	Menambahkan `Severity.Original` atribut, yang merupakan tingkat keparahan asli dari penyedia pencarian . Ini menggantikan atribut yang tidak digunakan lagi. `Severity.Product`	20 Mei 2020
Ob `Compliance.StatusReasons` jek baru di ASFF untuk detail tentang status kontrol	Menambahkan `Compliance.StatusReasons` objek, yang menyediakan konteks tambahan untuk status kontrol saat ini.	20 Mei 2020

Standar AWS Praktik Terbaik Keamanan Dasar Baru	Menambahkan standar AWS Praktik Terbaik Keamanan Dasar yang baru, yang merupakan serangkaian kontrol yang mendeteksi kapan akun dan sumber daya yang digunakan menyimpang dari praktik terbaik keamanan.	22 April 2020
Opsi konsol baru untuk memperbarui status alur kerja untuk temuan	Menambahkan informasi untuk menggunakan konsol Hub Keamanan atau API untuk mengatur status alur kerja untuk temuan.	16 April 2020
`BatchUpdateFindings` API baru untuk pembaruan pelanggan terhadap temuan	Menambahkan informasi tentang penggunaan `BatchUpdateFindings` untuk memperbarui informasi terkait dengan proses penyelidikan temuan. `BatchUpdateFindings` menggantikan`UpdateFindings`, yang tidak digunakan lagi.	16 April 2020

Pembaruan untuk Format Pen AWS emuan Keamanan (ASFF)	Menambahkan beberapa jenis sumber daya baru. Menambahkan `Label` atribut baru ke `Severity` objek. `Label`dimaksudkan untuk menggantikan `Normalize d` lapangan. Menambahkan `Workflow` objek baru untuk melacak proses penyelidi kan ke dalam temuan. `Workflow`berisi `Status` atribut, yang menggantikan `Workflowstate` atribut yang ada.	12 Maret 2020
Pembaruan pada halaman Integrasi	Diperbarui untuk mencermin kan perubahan pada halaman Integrasi. Untuk setiap integrasi, halaman sekarang menunjukkan kategori integrasi dan apakah setiap integrasi mengirimkan temuan ke atau menerima temuan dari Security Hub CSPM. Ini juga menyediakan langkah-langkah spesifik yang diperlukan untuk mengaktifkan setiap integrasi.	26 Februari 2020
Integrasi produk pihak ketiga baru	Menambahkan integrasi produk baru berikut: Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoin t DLP, Forcepoint NGFW, Rackspace Cloud Native Security, dan Cognito Detect. Vectra.ai	Februari 21, 2020

Standar keamanan baru untuk Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)	Menambahkan standar keamanan Security Hub CSPM untuk Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS). Ketika standar ini diaktifkan, Security Hub CSPM melakukan pemeriksaan otomatis terhadap kontrol yang terkait dengan persyaratan PCI DSS.	13 Februari 2020
Pembaruan untuk Format Pen AWS emuan Keamanan (ASFF)	Menambahkan bidang untuk persyaratan terkait untuk kontrol standar. Menambahk an jenis sumber daya baru dan detail sumber daya baru. ASFF juga sekarang memungkinkan Anda untuk menyediakan hingga 32 sumber daya.	5 Februari 2020
Opsi baru untuk menonakti fkan kontrol standar keamanan individu	Menambahkan informasi tentang cara mengontrol apakah setiap kontrol standar keamanan individu diaktifkan.	15 Januari 2020
Pembaruan untuk konsep CSPM Security Hub	Memperbarui beberapa deskripsi dan menambahk an istilah baru ke konsep Security Hub CSPM.	21 September 2019
AWS Security Hub CSPM rilis ketersediaan umum	Pembaruan konten untuk mencerminkan peningkatan yang dilakukan pada Security Hub CSPM selama periode beta.	25 Juni 2019

Menambahkan langkah-langkah remediasi untuk pemeriksaan Yayasan AWS CIS	Menambahkan langkah-langkah remediasi ke Standar Keamanan Didukung di AWS Security Hub C SPM.	April 15, 2019
rilis beta dari AWS Security Hub CSPM	Menerbitkan versi rilis beta dari Panduan AWS Pengguna CSPM Security Hub.	18 November 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.