사용 설명서

# AWS Security Hub



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

# AWS Security Hub: 사용 설명서

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

Amazon의 상표 및 트레이드 드레스는 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

# Table of Contents

Security Hub 및 Security Hub CSPM이란 무엇입니까? ..... 1
AWS Security Hub ..... 2
특성 ..... 2
통합 ..... 3
Security Hub에 액세스 ..... 3
개념 ..... 4
비용 예측기 ..... 9
계정 유형별 액세스 ..... 9
사전 조건 ..... 10
교차 계정 액세스 설정 ..... 11
비용 예측기 사용 ..... 14
중요 정보 ..... 21
관련 정보 ..... 22
Security Hub 활성화 ..... 22
AWS 조직에 대한 Security Hub 활성화 ..... 22
독립형 계정에서 Security Hub 활성화 ..... 25
위임 관리자 지정 ..... 26
위임된 관리자 정책 생성 ..... 27
멤버 계정의 구성 관리 ..... 28
위임 관리자 제거 ..... 32
Security Hub 다시 활성화 ..... 33
권장 사항 ..... 34
계정 적용 범위 ..... 35
계정 적용 범위 페이지 ..... 35
보안 적용 범위 위젯 ..... 37
확장 계획 ..... 37
확장 계획에 대한 권한 ..... 37
확장 플랜 파트너 가입 ..... 38
파트너 구독 취소 ..... 38
교차 리전 집계 ..... 39
집계되는 데이터 유형 ..... 39
관리자 및 멤버 계정의 집계 ..... 41
자동화 규칙 및 교차 리전 집계 ..... 41
집계 활성화 ..... 41

집계 설정 검토 ..... 42
집계 설정 업데이트 ..... 43
집계 삭제 ..... 44
Azure와 통합 ..... 44
AWS Config 를 사용하는 방법 ..... 46
추가 정보 ..... 46
사전 조건 ..... 47
Azure 구성 ..... 49
Security Hub 구성 ..... 59
Azure 커넥터 삭제 ..... 71
요약 대시보드 ..... 72
고려 사항 ..... 72
사용 가능한 위젯 ..... 73
사용 가능한 필터 ..... 86
Security Hub에서 리소스 세부 정보 보기 ..... 87
결과 형식: OCSF ..... 88
OCSF 개요 ..... 88
관련 리소스 ..... 89
AWS OCSF 확장 ..... 89
적용 범위 조사 결과 ..... 111
AWS Security Hub CSPM에 대한 적용 범위 조사 결과 ..... 112
Amazon GuardDuty의 적용 범위 조사 결과 ..... 112
Amazon Inspector의 적용 범위 조사 결과 ..... 113
Amazon Macie의 적용 범위 조사 결과 ..... 113
적용 범위 조사 결과 억제 ..... 113
AI 인벤토리 ..... 114
자체 호스팅 AI 검색을 위한 사전 조건 ..... 114
지원되는 AI 리소스 유형 ..... 115
리소스 페이지에서 AI 리소스 찾기 ..... 115
AI 인벤토리 페이지 사용 ..... 116
고려 사항 ..... 117
API를 사용하여 AI 인벤토리에 액세스 ..... 117
노출 조사 결과 ..... 119
노출 조사 결과의 작동 방식 ..... 119
노출 조사 결과의 구성 요소 ..... 120
심각도 분류 ..... 122

노출 조사 결과의 이점 ..... 122
노출 조사 결과의 출처 ..... 122
모범 사례 ..... 123
지원되는 리소스 ..... 123
지원되는 특성 ..... 124
노출 조사 결과 생성 ..... 127
노출 조사 결과의 심각도 수준 결정 ..... 131
노출 조사 결과 검토 ..... 133
잠재적 공격 경로 그래프 ..... 135
노출 조사 결과 문제 해결 ..... 135
미사용 액세스 조사 결과 ..... 228
미사용 액세스 분석 작동 방식 ..... 228
미사용 액세스 조사 결과 유형 ..... 228
서비스 연결 분석기 ..... 229
미사용 액세스 조사 결과 보기 ..... 229
노출 조사 결과의 미사용 액세스 ..... 230
미사용 권한에 대한 정책 권장 사항 ..... 230
가격 책정 ..... 230
정책 권장 사항 ..... 230
정책 권장 사항의 작동 방식 ..... 230
추천을 생성할 수 있는 사용자 ..... 231
권장 사항 수명 주기 ..... 231
오류 사례 ..... 232
콘솔 사용 ..... 232
API 참조 ..... 232
네트워크 스캔 ..... 233
지원되는 리소스 유형 ..... 233
네트워크 스캔 활성화 ..... 234
네트워크 스캔 작동 방식 ..... 235
네트워크 스캔 조사 결과 ..... 235
스캔 증거 ..... 238
스캔에서 리소스 제외 ..... 238
지원되는 포트 ..... 239
다중 클라우드 지원 ..... 239
리전 가용성 ..... 239
네트워크 스캔 비활성화 ..... 239

자동화 ..... 240
자동화 규칙 ..... 241
EventBridge 자동화 규칙 ..... 259
타사 통합 ..... 3
Jira Cloud ..... 268
ServiceNow ..... 273
티켓팅 통합을 위한 KMS 키 정책 ..... 280
티켓팅 통합 테스트 ..... 283
MCP 앱(미리 보기) ..... 285
MCP 앱 예제 ..... 286
주요 개념 ..... 289
사전 조건 ..... 290
MCP 서버 설정 ..... 290
커넥터 진단 사용 ..... 291
사용 가능한 도구 ..... 292
사용량 및 비용 모니터링 ..... 293
사용 페이지에 액세스할 수 있는 사용자 ..... 293
조직 및 계정 비용 요약 ..... 293
기능 보기 ..... 294
계정 보기 ..... 295
비용 최적화 전략 ..... 296
관련 리소스 ..... 296
Security Hub 비활성화 ..... 296
단일 계정에 대해 Security Hub 비활성화 ..... 296
조직 전체에서 Security Hub 비활성화 ..... 297
보안 ..... 299
데이터 보호 ..... 300
ID 및 액세스 관리 ..... 302
규정 준수 확인 ..... 331
복원력 ..... 332
인프라 보안 ..... 332
VPC 엔드포인트(AWS PrivateLink) ..... 332
API 직접 호출 로깅 ..... 334
CloudTrail의 Security Hub 정보 ..... 334
예제: Security Hub의 로그 파일 항목 ..... 335
AWS Security Hub CSPM ..... 339

Security Hub CSPM의 이점 ..... 340
Security Hub CSPM 액세스 ..... 341
관련 서비스 ..... 342
Security Hub CSPM 무료 평가판, 사용량 및 요금 ..... 343
사용 세부 정보 보기 ..... 343
요금 내역 ..... 343
개념 ..... 343
Security Hub CSPM 활성화 ..... 349
필요한 권한 확인 ..... 349
Organizations 통합을 통해 Security Hub CSPM 활성화 ..... 349
수동으로 Security Hub CSPM 활성화 ..... 351
다음 단계: 태세 관리 및 통합 ..... 353
구성 AWS Config ..... 353
로컬 구성 ..... 359
중앙 구성 ..... 360
다중 계정 관리 ..... 401
를 사용하여 계정 관리AWS Organizations ..... 401
초대를 통한 수동 계정 관리 ..... 402
다중 계정 환경에 대한 권장 사항 ..... 402
를 사용하여 계정 관리AWS Organizations ..... 404
초대를 통한 계정 관리 ..... 418
관리자 및 멤버 계정에서 허용되는 작업 ..... 431
계정 작업이 데이터에 미치는 영향 ..... 436
리전 간 데이터 집계 ..... 439
집계되는 데이터 유형 ..... 440
관리자 및 멤버 계정의 집계 ..... 441
중앙 구성 및 집계 ..... 442
집계 활성화 ..... 443
집계 설정 검토 ..... 445
집계 설정 업데이트 ..... 446
집계 중지 ..... 448
표준 ..... 449
표준 참조 ..... 450
표준 활성화 ..... 535
표준 세부 정보 검토 ..... 541
자동 활성화 표준 끄기 ..... 544

표준 비활성화 ..... 545
제어 ..... 547
통합 제어 보기 ..... 548
제어에 대한 요약 보안 점수 ..... 549
제어 참조 ..... 549
제어를 구성하기 위한 권한 ..... 1349
제어 활성화 ..... 1349
제어 비활성화 ..... 1357
보안 검사 및 점수 ..... 1367
제어 범주 ..... 1441
제어의 세부 정보 검토 ..... 1444
제어 필터링 및 정렬 ..... 1447
제어 파라미터 ..... 1448
제어 조사 결과 검토 및 관리 ..... 1460
통합 ..... 1488
통합 목록 검토 ..... 1489
통합에서 조사 결과의 흐름 활성화 ..... 1490
통합에서 조사 결과의 흐름 비활성화 ..... 1492
통합에서 조사 결과 보기 ..... 1492
AWS 서비스 통합 ..... 1493
타사 통합 ..... 1514
사용자 지정 제품 통합 ..... 1547
Azure와 통합 ..... 1549
AWS Config 를 사용하는 방법 ..... 1551
커넥터 유형 ..... 1551
사전 조건 ..... 1552
Azure 구성 ..... 1554
Security Hub CSPM 구성 ..... 1560
Azure 커넥터 삭제 ..... 1579
조사 결과 ..... 1580
조사 결과 공급자에 대한 BatchImportFindings ..... 1582
고객에 대한 BatchUpdateFindings ..... 1585
조사 결과 세부 정보 및 기록 검토 ..... 1589
조사 결과 필터링 ..... 1593
조사 결과 그룹화 ..... 1596
조사 결과에 대한 워크플로 상태 설정 ..... 1597

사용자 지정 작업에 조사 결과 전송 ..... 1599
조사 결과 형식: ASFF ..... 1600
인사이트 ..... 1890
인사이트 검토 및 조치 ..... 1891
관리형 인사이트 ..... 1893
사용자 지정 인사이트 ..... 1904
자동화 ..... 1911
자동화 규칙 ..... 1912
자동 응답 및 해결 ..... 1937
요약 대시보드 ..... 1953
요약 대시보드에 사용할 수 있는 위젯 ..... 1953
대시보드 필터링 ..... 1957
대시보드 사용자 지정 ..... 1959
리전 제한 ..... 1959
교차 리전 집계 제한 ..... 1959
리전별 통합 사용 가능 여부 ..... 1960
리전별 표준 사용 가능 여부 ..... 1962
리전별 제어 기능 사용 가능 여부 ..... 1962
제어 기능에 대한 리전별 제한 ..... 1963
CloudFormation을 사용하여 리소스 생성 ..... 2211
Security Hub CSPM 및 CloudFormation템플릿 ..... 2212
에 대해 자세히 알아보기CloudFormation ..... 2212
공지 구독 ..... 2213
Amazon SNS 메시지 형식 ..... 2218
Security Hub CSPM 비활성화 ..... 2220
보안 ..... 2222
데이터 보호 ..... 2223
ID 및 액세스 관리 ..... 2224
규정 준수 확인 ..... 2255
복원력 ..... 2256
인프라 보안 ..... 2256
VPC 엔드포인트(AWS PrivateLink) ..... 2256
API 직접 호출 로깅 ..... 2258
CloudTrail의 Security Hub CSPM 정보 ..... 334
예제: Security Hub CSPM 로그 파일 항목 ..... 335
리소스에 태그 지정 ..... 2262

태그 지정 기본 사항 ..... 2262
IAM 정책에서 태그 사용 ..... 2263
리소스에 태그 추가 ..... 2264
리소스에 대한 태그 편집 ..... 2267
리소스에 대한 태그 검토 ..... 2269
리소스에서 태그 제거 ..... 2271
할당량 ..... 2273
최대 할당량 ..... 2273
비율 할당량 ..... 2273
문서 기록 ..... 2274
..... mmccclxxiii

# Security Hub 및 Security Hub CSPM이란 무엇입니까?

AWSSecurity Hub 및 AWSSecurity Hub CSPM은 클라우드 환경을 AWS 서비스보호합니다. 이들 서비스는 서로 보완합니다. 함께 사용하면 AWS환경의 보안 태세에 대한 귀중한 인사이트를 얻을 수 있습니다.

Security Hub CSPM은 보안 태세에 대한 포괄적인 관점을 제공하며, 보안 업계 표준 및 모범 사례와 비교하여 클라우드 환경을 평가하는 데 도움이 됩니다. Security Hub는 중요한 보안 문제의 우선순위를 지정하고 이에 대응하는 데 도움이 되는 통합 환경을 제공합니다. Security Hub CSPM 조사 결과는 자동으로 Security Hub로 라우팅되며, 여기서 Amazon Inspector와 같은 다른 보안 서비스의 조사 결과와 상호 연관되어 노출을 생성합니다. 이를 통해 환경에서 가장 중요한 위험을 식별할 수 있습니다. 또한 Security Hub는 Security Hub CSPM 조사 결과를 운영 워크플로에 통합할 수 있는 자동 워크플로 기능을 제공합니다.

모범 사례로 두 서비스를 모두 활성화하는 것이 좋습니다. 잘못된 구성을 식별하고 보안 태세를 평가하는 것이 주된 목적이라면 Security Hub를 활성화하지 않고 Security Hub CSPM만 활성화할 수 있습니다. 하지만 Security Hub CSPM을 활성화하지 않고 Security Hub를 활성화하면 Security Hub가 Security Hub CSPM 조사 결과를 사용하여 AWS 환경의 위험 및 노출에 대한 정보를 제공할 수 없습니다. 최적의 환경을 위해 Security Hub와 Security Hub CSPM을 활성화할 뿐만 아니라 Amazon GuardDuty, Amazon Inspector, Amazon Macie와 같은 다른 보안 서비스도 활성화하는 것이 좋습니다.

# AWS Security Hub 소개

AWS Security Hub는 중요한 보안 문제를 우선시하고 대규모로 대응하는 데 도움이 되는 통합 클라우드 보안 솔루션입니다. Security Hub는 여러 소스의 보안 신호를 자동으로 상호 연관시키고 보강하여 보안 문제를 감지합니다. 이러한 소스에는 태세 관리, 취약성 관리(Amazon Inspector), 민감한 데이터(Amazon Macie) 및 위협 탐지(Amazon GuardDuty)가 포함됩니다. Security Hub를 사용하면 자동화된 분석 및 컨텍스트 인사이트를 통해 클라우드 환경의 활성 위험을 우선시할 수 있습니다. 직관적인 시각화를 통해 Security Hub는 복잡한 보안 신호를 실행 가능한 인사이트로 변환하므로 정보에 입각한 보안 결정을 신속하게 내릴 수 있습니다. Security Hub에는 위험을 해결하고, 팀 생산성을 개선하고, 운영 중단을 최소화하는 데 도움이 되는 자동 응답 워크플로도 포함되어 있습니다.

## 특성

통합 보안 솔루션

통합 클라우드 보안 솔루션에서의 중앙 집중식 관리를 통해 클라우드 환경 전체에서 더 광범위한 가시성을 확보합니다.

실행 가능한 보안 인사이트

고급 분석을 통해 환경과 관련된 보안 위험을 파악하여 실행 가능한 보안 인사이트를 얻습니다.

대응 시간 단축

자동화된 워크플로와 통합 티켓팅 시스템으로 대응 시간을 효율화합니다.

노출 조사 결과

Security Hub는 Security Hub CSPM 제어 검사, Amazon Inspector 및 기타의 조사 결과를 상호 연관 AWS 서비스 시켜 AWS 리소스와 관련된 노출을 탐지합니다.

미사용 액세스 분석

Security Hub는 90일 룩백 기간 내에 사용되지 않은 IAM 역할, 사용자, 액세스 키 및 권한을 자동으로 식별합니다. Security Hub를 활성화하면 서비스가 계정에 서비스 연결 IAM Access Analyzer를 생성합니다. 미사용 액세스 조사 결과는 과다 프로비저닝된 IAM 보안 주체를 강조 표시하여 최소 권한 액세스를 구현하는 데 도움이 됩니다. 미사용 권한 조사 결과의 경우 Security Hub는 범위가 축소된 대체 정책을 보여주는 최소 권한 정책 권장 사항을 생성할 수 있습니다.

조사 결과는 개방형 사이버 보안 스키마 프레임워크(OCSF) 형식이 지정됩니다

Security Hub는 OCSF에서 결과를 생성하고 Security Hub CSPM 및 기타로부터 OCSF에서 결과를 수신합니다 AWS 서비스.

- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector –

대시보드

Security Hub 콘솔은 노출, 위협, 보안 범위 및 리소스에 대한 포괄적인 보기, 그리고 잠재적 공격자가 노출 조사 결과와 연결된 리소스에 액세스하고 제어하는 방법을 보여주는 공격 경로 그래프라는 대화형 시각화를 제공합니다.

서드 파티 제품과의 통합

Security Hub 통합을 통해 보안 태세를 강화할 수 있습니다. 예를 들어 Jira Cloud 또는 ServiceNow ITSM을 사용하는 경우 이 기능을 사용하여 조사 결과에서 티켓을 생성할 수 있습니다.

## 통합

Security Hub는 다음과 같은 결과를 수신합니다 AWS 서비스.

- AWS Security Hub CSPM
- Amazon GuardDuty
- Amazon Inspector –
- Amazon Macie
- IAM Access Analyzer

# Security Hub에 액세스

Security Hub는 대부분의 AWS 리전에서 사용할 수 있습니다. 현재 Security Hub를 사용할 수 있는 리전 목록은 AWS 일반 참조의 Security Hub 엔드포인트 및 할당량을 참조하세요. 에 AWS 리전 대한 관리에 대한 자세한 AWS 계정내용은 AWS Account Management 참조 안내서의 계정에서 사용할 수 있는 지정을 참조 AWS 리전하세요.

조직의 개별 계정 또는 계정에 대해 Security Hub를 활성화할 수 있습니다. 각 리전에서는 다음 방법 중 하나를 사용하여 Security Hub에 액세스하여 사용할 수 있습니다.

Security Hub 콘솔

Security Hub 콘솔은 AWS 리소스를 생성하고 관리하는 데 사용할 수 있는 브라우저 기반 인터페이스입니다. 이 콘솔에서 계정, 데이터, 리소스에 액세스할 수 있습니다.

Security Hub API

Security Hub API를 사용하면 프로그래밍 방식으로 계정, 데이터, 리소스에 액세스할 수 있습니다. HTTPS 요청을 Security Hub에 직접 보낼 수 있습니다.

AWS CLI

를 AWS CLI 사용하면 시스템 명령줄에서 명령을 실행하여 작업을 수행하고 작업을 수행하는 스크립트를 빌드할 수 있습니다. 경우에 따라가 Security Hub 콘솔보다 더 유용할 AWS CLI 수 있습니다.

AWS SDKs

AWS SDKs 다양한 프로그래밍 언어 및 플랫폼(C++, Go, Java, .NET 및 Python)을 위한 라이브러리와 샘플 코드로 구성됩니다. 원하는 언어로 Security Hub 및 기타 AWS 서비스 에 프로그래밍 방식으로 액세스할 수 있으며 오류 관리, 요청 서명, 요청 재시도와 같은 작업을 관리하는 데 도움이 될 수 있습니다.

# Security Hub 개념

Security Hub에서는 일반적인 AWS 개념과 용어를 기반으로 이러한 추가 용어를 사용합니다.

Account

AWS 리소스가 포함된 표준 AWS 계정입니다. AWS AWS 계정으로에 로그인하여 Security Hub를 활성화합니다.

계정이에 등록된 경우 AWS Organizations조직에서 Security Hub 관리자 계정을 지정합니다. 이 계정은 다른 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

조직은 관리자 계정을 1개만 보유할 수 있습니다. 한 계정이 관리자 계정이면서 동시에 멤버 계정일 수 없습니다.

Security Hub는 다음 계정을 지원합니다.

- 조직 관리 계정 - AWS 조직을 관리하는 AWS 계정입니다.
- 위임된 관리자 계정 - AWS 조직의 사용을 관리하는 AWS 계정 AWS 서비스 입니다.
- 멤버 계정 - AWS 조직의 멤버인 AWS 계정입니다.

- 독립 실행형 계정 - AWS Organizations 활성화되지 않은 AWS 계정입니다.

관리자 계정

이 유형의 AWS 계정은 연결된 멤버 계정에 대한 조사 결과를 볼 수 있습니다.

이 유형의 AWS 계정은 조직 관리 계정이 Security Hub 관리자 계정으로 지정한 경우 관리자 계정이 됩니다. Security Hub 관리자 계정은 모든 조직 계정을 멤버 계정으로 활성화할 수 있으며 다른 계정을 멤버 계정으로 초대할 수도 있습니다.

조직은 관리자 계정을 1개만 보유할 수 있습니다. 한 계정이 관리자 계정이면서 동시에 멤버 계정일 수 없습니다.

집계 리전

집계 리전을 사용하면 단일 창에서 여러의 보안 결과를 볼 AWS 리전 수 있습니다.

집계 리전은 조사 결과를 보고 관리하는 AWS 리전 입니다. 조사 결과는 연결된 리전에서 집계 영역으로 집계됩니다. 업데이트된 조사 결과는 리전 전체에 복제됩니다.

집계 영역의 대시보드 및 인벤토리 페이지에는 모든 연결된 리전의 데이터가 포함됩니다. 자동화 페이지는 집계 영역에서 자동화 규칙을 정의하는 데만 사용할 수 있습니다. 서드 파티 티켓팅 통합은 집계 영역에서만 구성할 수 있습니다.

보관된 조사 결과

상태가 `ARCHIVED`인 조사 결과입니다. 이러한 조사 결과는 조사 결과를 조사하는 조사 결과 공급자 또는 고객이 해당 조사 결과가 더 이상 관련성이 없다고 판단한다는 것을 나타냅니다.

조사 결과 공급자는 자신이 생성한 조사 결과를 보관할 수 있습니다. 고객은 Security Hub API의 BatchUpdateFindingsV2 작업을 사용하거나 Security Hub 콘솔에서 상태를 업데이트하여 더 이상 관련이 없다고 생각되는 모든 결과를 보관할 수 있습니다.

Security Hub 콘솔의 기본 필터 설정은 조사 결과 목록 및 테이블에서 보관된 결과를 제외합니다. 보관된 조사 결과를 포함하도록 필터를 업데이트할 수 있습니다. GetFindingsV2 작업을 사용하여 조사 결과를 검색하면 작업은 보관된 조사 결과와 활성 조사 결과를 모두 검색합니다. 다음 예제에서는 결과에서 보관된 조사 결과를 제외하는 방법을 보여줍니다.

```
{
    "StringFilters":
    [
        {
            "FieldName": "status",
            "Filter":
```

```
            {
                "Value": "Archived",
                "Comparison": "EQUALS"
            }
        }
    ]
}
```

교차 리전 집계

조사 결과 및 리소스가 연결된 리전에서 집계 영역으로 집계됩니다. 집계 영역에서 모든 데이터를 보고 조사 결과를 업데이트할 수 있습니다.

위임된 관리자 계정

에서 서비스의 AWS Organizations위임된 관리자 계정은 조직의 서비스 사용을 관리할 수 있습니다.

Security Hub에서 Security Hub 관리자 계정은 Security Hub의 위임된 관리자 계정이기도 합니다. 조직 관리 계정이 Security Hub 관리자 계정을 처음 지정하면 Security Hub가 조직을 호출하여 해당 계정을 위임된 관리자 계정으로 설정합니다.

그런 다음에는 조직 관리 계정이 모든 리전에서 Security Hub 관리자 계정으로 위임된 관리자 계정을 선택해야 합니다.

Exposure

노출이란 보안 제어, 잘못된 구성 또는 활성 위협으로 악용될 수 있는 기타 영역의 광범위한 약점입니다.

노출의 예는 다음과 같습니다.

- 리소스에 대해 잘못 구성된 컨트롤 플레인입니다.
- 악용 가능성이 높은 소프트웨어 취약성이 있습니다.
- 공개적으로 액세스할 수 있는 리소스(네트워크 또는 API).

노출 조사 결과

환경에 존재하는 노출을 설명하는 조사 결과의 유형입니다. 노출 조사 결과에는 특성과 신호가 포함됩니다. 신호에는 여러 유형의 노출 특성이 포함될 수 있습니다. AWS Security Hub는 AWS Security Hub CSPM, Amazon Inspector, Amazon GuardDuty, Amazon Macie 또는 기타 AWS 서비스의 신호가 노출 여부를 나타낼 때 노출 결과를 생성합니다. 리소스는 하나 이상의 노출 결과에 관여할 수 있습니다. 리소스에 노출 특성이 없거나 특성이 부족한 경우 Security Hub는 해당 리소스에 대한 노출 결과를 생성하지 않습니다.

노출 결과의 예로는 인터넷에서 연결할 수 있고 악용 가능성이 높은 소프트웨어 취약성이 있는 EC2 인스턴스가 있습니다.

조사 결과

보안 점검 또는 보안 관련 감지의 관찰 가능한 기록입니다. Security Hub는 다른 보안 조사 결과의 상관관계를 통해 조사 결과를 생성하고 업데이트합니다. 이를 노출 조사 결과라고 합니다. 조사 결과는 다른 AWS 서비스 및 타사 제품과의 통합에서도 얻을 수 있습니다.

조사 결과 수집

조사 결과를 Security Hub로 가져오는 것입니다. 조사 결과 수집 이벤트에는 새로운 조사 결과와 기존의 조사 결과에 대한 업데이트가 모두 포함됩니다.

연결된 리전

교차 리전 집계를 활성화하면 연결된 리전은 조사 결과 및 리소스 인벤토리를 집계 영역으로 집계하는 리전입니다.

연결된 리전에서 대시보드 및 인벤토리 페이지에는 이에 대한 조사 결과만 포함됩니다 AWS 리전.

개방형 사이버 보안 스키마 프레임워크(OCSF)

Open Cybersecurity Schema Framework(OCSF)는 사이버 보안 업계의 AWS 및 주요 파트너가 공동으로 수행하는 오픈 소스 작업입니다. OCSF는 일반적인 보안 이벤트에 대한 표준 스키마를 제공하고, 스키마 진화를 촉진하기 위한 버전 관리 기준을 정의하며, 보안 로그 생성자와 소비자를 위한 자체 거버넌스 프로세스를 포함합니다. 자세한 내용은 Security Hub의 OCSF 조사 결과를 참조하세요.

멤버 계정

관리자 계정에 조사 결과를 보고 조치를 취할 수 AWS 계정 있는 권한을 부여한 입니다. 이러한 종류의 AWS 계정 는 Security Hub 관리자 계정이 멤버 계정으로 활성화할 때 멤버 계정이 됩니다.

신호

노출 조사 결과에 기여하는 조사 결과입니다. 신호를 기여 조사 결과라고 할 수 있습니다. 신호는 Security Hub CSPM AWS Config또는 Amazon Inspector AWS 서비스와 같은 기타에서 발생할 수 있습니다.

서비스 연결 구성 레코더

서비스별 리소스에 대한 구성 데이터를 기록하는 데 사용되는 AWS Config 레코더 유형입니다. Security Hub는 이벤트 기반 접근 방식으로 이러한 레코더를 사용하여 노출 분석 적용 범위, 리소스 인벤토리 보고 및 태세 관리 제어 평가를 위한 리소스 구성 항목을 가져옵니다. 이 기능은 Essential

플랜 요금의 일부로 모든 Security Hub 고객에게 제공됩니다. Security Hub를 활성화하면 계정에 다음과 같은 서비스 연결 구성 레코더가 생성됩니다.

- 각 AWS 계정 및 에는 이름이 AWS 리전인 서비스 연결 구성 레코더`AWSConfigurationRecorderForSecurityHubAssets`가 생성됩니다.
- 글로벌 리소스 유형의 경우 이름이 인 추가 서비스 연결 구성 레코더`AWSConfigurationRecorderForSecurityHubAssetsGlobal`가 us-east-1에 생성됩니다 AWS 리전.
- Security Hub와 Security Hub CSPM이 모두 AWS 계정 및에서 활성화된 경우 이름이 AWS 리전인 서비스 연결 구성 레코더`AWSConfigurationRecorderForSecurityHubCSPM`가 생성됩니다.

자세한 내용은 서비스 연결 구성 레코더에 대한 고려 사항 및 리전 및 글로벌 리소스 기록을 참조하세요.

서비스 연결 분석기

Security Hub가 사용자를 대신하여 생성하고 관리하는 IAM Access Analyzer입니다. Security Hub를 활성화하면 서비스 연결 미사용 액세스 분석기가 자동으로 생성되어 90일 룩백 기간 내에 사용되지 않은 IAM 역할, 사용자, 액세스 키 및 권한을 식별합니다. IAM은 글로벌 서비스이므로 분석기는 미국 동부(버지니아 북부)에서 실행됩니다. Security Hub는 Security Hub를 활성화한 모든 리전에 미사용 액세스 조사 결과를 복제합니다. IAM Access Analyzer를 별도로 활성화하거나 추가 조치를 취할 필요가 없습니다. 이 기능은 Essential 플랜 요금의 일부로 모든 Security Hub 고객에게 제공됩니다. 서비스 연결 분석기는 IAM Access Analyzer 콘솔에서 볼 수 있지만 Security Hub가 활성화된 동안에는 수정하거나 삭제할 수 없습니다. Security Hub는의 모든 리전에서 서비스를 비활성화하면 분석기를 삭제합니다 AWS 계정. 자세한 내용은 the section called “미사용 액세스 조사 결과” 단원을 참조하십시오.

특성

노출 조사 결과를 초래하는 보안 편차입니다. 특성 유형에는 수임 가능성, 잘못된 구성, 연결성, 민감한 데이터 및 취약성이 포함됩니다. 특성은 하나의 신호와 연결되며 각 신호에는 여러 특성이 포함될 수 있습니다. 예를 들어 Security Hub CSPM 제어는 고객 관리형 정책이 관리 액세스 제어를 허용함을 나타냅니다. 이 신호에는 잘못된 구성 특성이 포함되어 있습니다.

미사용 액세스 조사 결과

90일 룩백 기간 내에 사용되지 않은 IAM 역할, 사용자, 액세스 키 또는 권한 세트를 식별하는 결과입니다. Security Hub는 서비스 연결 IAM Access Analyzer를 사용하여 미사용 액세스 조사 결과를 생성합니다. 미사용 액세스 조사 결과에는 미사용 IAM 역할, 미사용 IAM 사용자 액세스 키, 미사용 IAM 사용자 암호, 미사용 권한의 네 가지 유형이 있습니다.

# AWS Security Hub Cost Estimator

Security Hub 비용 예측기는 AWS 환경 전반의 Security Hub 기능에 대한 추정치를 제공하는 콘솔 기능입니다. 비용 예측기는 AWS Security Hub의 간소화된 요금제를 사용하여 Security Hub CSPM, Amazon Inspector 및 Amazon GuardDuty의 개별 서비스 비용과 Security Hub의 예상 비용을 보여줍니다. 예상 사용량과 리소스 수를 AWS 사용량에 맞게 조정하여 예상 정확도를 높일 수 있습니다. 비용 예측기는 Security Hub를 사용할 수 있는 모든 리전에서 사용할 수 있습니다.

비용 예측기는 두 가지 요금 모델을 사용하여 보안 기능에 대한 월별 비용을 추정합니다.

- 개별 서비스 요금 - 각 보안 기능에 대해 별도로 지불합니다(GuardDuty, Amazon Inspector, Security Hub CSPM).
- Security Hub 간소화된 요금 - 3가지 요금제, 리소스별 요금이 적용되는 필수 요금제, 이벤트별 및 GB당 로그 요금이 적용되는 위협 분석, 리소스별 요금이 적용되는 Lambda 코드 스캔의 통합 요금제.

예측기는 사용 가능한 경우 AWS Cost Explorer 데이터를 사용합니다. Cost Explorer 데이터를 사용할 수 없는 경우 사용량 데이터를 수동으로 입력할 수 있습니다. 예상 비용은 관찰된 사용량과 사용자가 제공한 사용량 및 공개 요금 정보를 기반으로 합니다. 견적에는 엔터프라이즈 할인이 반영되지 않을 수 있습니다.

비용 예측기의 주요 이점은 다음과 같습니다.

- Security Hub를 활성화할 때 통합 요금의 비용이 Security Hub를 활성화하지 않고 개별 서비스와 어떻게 비교되는지 확인합니다.
- 기능을 활성화하기 전에 비용 추정
- 사용량 파라미터를 조정하여 다양한 시나리오 모델링
- 이해관계자 검토를 위해 견적을 PDF로 내보내기

## 계정 유형별 액세스

> **Note**
>
> 위임된 관리자 및 멤버 계정의 경우 기본적으로 비용 예측기가 편집 모드로 열리므로 사용 데이터를 즉시 입력할 수 있습니다. 관리 계정과 독립 실행형 계정은 Cost Explorer 데이터를 사용할 수 있을 때 보기 모드에서 열립니다.

이 기능은 실제 과거 사용량에 대한 정보를 자동으로 검색하여 특정 계정 유형에 대한 비용을 추정합니다. 각 계정 유형과 각 계정 유형에 사용할 수 있는 데이터에 대한 자세한 내용은 다음 표를 참조하세요.

계정 유형별 액세스 권한

| 계정 유형 | Cost Explorer 데이터 | 데이터 입력 | Scope |
|---|---|---|---|
| 관리 계정(MA) | 자동 채워짐 | 수동 재정의 사용 가능 | 조직 전체 |
| 위임된 관리자(DA) | 교차 계정 역할을 통해 자동 채워짐* | 수동 재정의 사용 가능 | 조직 전체 |
| 멤버 계정 | 교차 계정 역할을 통해 자동 채워짐* | 수동 재정의 사용 가능 | 조직 전체 |
| 독립 실행형 계정(SA) | 자동 채워짐 | 수동 재정의 사용 가능 | 단일 계정 |

* 관리 계정에서 교차 계정 IAM 역할 구성이 필요합니다. 아래 교차 계정 액세스 설정 섹션을 참조하세요.

# 사전 조건

## 필수 IAM 권한

비용 예측기의 모든 기능을 사용하려면 IAM 보안 주체에 다음 권한이 있어야 합니다.

Cost Estimator에 필요한 IAM 권한

| API 작업 | 서비스 | 용도 |
|---|---|---|
| `ce:GetCostAndUsage` | AWS Cost Explorer | 과거 사용량 및 비용 데이터 검색 |
| `pricing:GetProducts` | AWS 요금 | 현재 요금 적용 |
| `organizations:ListAccounts` | AWS 조직 | 조직의 계정 수 계산 |
| `organizations:DescribeOrganization` | AWS 조직 | 계정 유형 결정 |

| API 작업 | 서비스 | 용도 |
| --- | --- | --- |
| `securityhub:ListOrganizationAdminAccounts` | Security Hub | 조직 관리자 계정 나열 |
| `iam:GetRole` | IAM | 교차 계정 역할 존재 확인(관리 계정만 해당)* |
| `sts:AssumeRole` | IAM | 교차 계정 역할 수임(위임된 관리자/멤버 계정만 해당)** |

* 관리 계정 사용자가 교차 계정 역할 상태를 확인하는 데에만 필요합니다.

** 교차 계정 액세스를 사용하는 위임된 관리자 및 조직 구성원 계정에만 필요합니다.

### 추가 요구 사항

Cost Explorer

자동 데이터 모집단(활성화 후 24시간 처리 지연)에 대해 활성화해야 합니다.

## 교차 계정 액세스 설정

위임된 관리자 및 멤버 계정은 교차 계정 IAM 역할을 구성하여 관리 계정에서 조직 전체의 AWS Cost Explorer 데이터에 액세스할 수 있습니다. 이 구성을 통해 이러한 계정은 관리 계정으로 전환하지 않고도 실제 사용 데이터를 볼 수 있습니다.

### 사전 조건

비용 예측기에 대한 교차 계정 액세스를 설정하기 전에 다음 항목과 정보가 필요합니다.

- 관리 계정이 AWS Cost Explorer 활성화되어 있어야 합니다.
- 관리 계정에서 역할을 생성할 수 있는 IAM 권한입니다.
- 교차 계정 액세스 권한이 부여될 위임된 관리자 또는 멤버 계정 ID에 대한 지식입니다.

## 설정 단계

비용 예측기는 콘솔에서 직접 안내 설정 지침을 제공합니다. 지침에 액세스하려면 조직 관리 계정의 https://console.aws.amazon.com/securityhub/v2/home#/costEstimator 비용 예측기 페이지로 이동합니다. 교차 계정 액세스 섹션을 찾아 교차 계정 역할을 설정하기 위해 설명된 단계를 따릅니다.

## 역할 구성

비용 예측기에 대한 교차 계정 액세스에는 신뢰 정책 및 권한 정책을 사용하여 IAM 역할을 설정해야 합니다. 교차 계정 역할은 다음 구성을 사용하여 관리 계정에서 생성해야 합니다.

역할 이름(정확한 이름 필요) - AwsSecurityHubCostEstimatorCrossAccountRole

권장 신뢰 정책:

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

정책 예제에서 다음 값을 대체하여 정책을 편집합니다.

- *{ACCOUNT_ID}*를 교차 계정 액세스 권한을 부여하는 위임된 관리자 또는 멤버 계정 ID로 바꿉니다.
- *{ROLE_NAME}*을 액세스 권한을 부여하려는 위임된 관리자 또는 멤버 계정의 IAM 역할 이름으로 바꿉니다.

권장 권한 정책:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "ce:GetCostAndUsage",
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> 신뢰 정책은 특정 계정 및 역할에 대한 액세스를 제한합니다. 지정된 IAM 보안 주체만이 역할을 수임하여 무단 액세스를 방지할 수 있습니다.

## Verification(확인)

관리 계정에서 역할을 생성한 후 다음 단계를 사용하여 설정이 작동하는지 확인합니다.

1. 위임된 관리자 또는 멤버 계정에 로그인합니다.
2. https://console.aws.amazon.com/securityhub/v2/home#/costEstimator Security Hub 비용 예측기로 이동합니다.
3. 페이지는 자동으로 다음을 수행해야 합니다.
    a. 조직의 관리 계정을 감지합니다.
    b. 교차 계정 역할을 수임합니다.
    c. 조직 전체 사용량으로 Cost Explorer 데이터를 로드합니다.

성공하면 수동 입력 필드 대신 실제 사용 데이터가 나타납니다.

## 문제 해결

이 섹션에서는 교차 계정 액세스를 설정할 때 발생할 수 있는 일반적인 문제와 해결 방법을 다룹니다.

이 계정에는 조직 사용량 데이터를 사용할 수 없습니다.

이 알림은 교차 계정 역할에 액세스할 수 없음을 나타냅니다. 이 알림의 가능한 원인은 다음과 같습니다.

1. 역할이 존재하지 않음: 관리 계정이 아직 역할을 생성하지 않았습니다.

- 해결 방법: 관리 계정 관리자에게 문의하여 설정 지침에 따라 역할을 생성합니다.

2. 역할 이름 불일치: 역할 이름이 정확히 일치하지 않습니다.

   - 해결 방법: 역할 이름이 인지 확인합니다`AwsSecurityHubCostEstimatorCrossAccountRole`.

3. 신뢰 정책이 올바르지 않음: 신뢰 정책은 계정이 역할을 수임하도록 허용하지 않습니다.

   - 해결 방법: 신뢰 정책에 계정 ID와 역할 이름이 포함되어 있는지 확인합니다.

4. AssumeRole 권한 누락: IAM 보안 주체에이 없습니다`sts:AssumeRole`.

   - 해결 방법: 관리자에게 문의하여 `sts:AssumeRole` 권한을 추가합니다.

자세한 설정 지침을 보려면: 알림에서 지침 보기를 선택하여 step-by-step 지침 및 정책 템플릿이 포함된 모달을 엽니다.

해결 방법: 편집 모드에서 사용량 값을 수동으로 입력하여 Cost Estimator를 계속 사용할 수 있습니다.

# 비용 예측기 사용

## 비용 예측기 액세스

Security Hub 랜딩 페이지에서 Cost Estimator에 액세스하려면

1. AWS 조직 관리 또는 위임된 관리자 AWS 계정 자격 증명을 사용하여 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home us-east-1 리전에서 Security Hub 콘솔을 엽니다.
2. 랜딩 페이지에서 요금 카드를 찾습니다.
3. 예상 비용을 선택합니다.

Security Hub 활성화 및 구성 단계에서 Cost Estimator에 액세스하려면

1. 온보딩 인터페이스의 새 Security Hub 카드에서 요금을 찾습니다.
2. 견적 보기를 선택합니다.

GuardDuty, Amazon Inspector 또는 Security Hub CSPM 콘솔에서 비용 예측기에 액세스하려면

1. 서비스 대시보드 또는 요약 페이지로 이동합니다.

2. 요금 정보 카드에서 요금 비교를 선택합니다.

## 비용 예측기 인터페이스 이해

### 페이지 레이아웃

Cost Estimator 페이지에는 세 가지 주요 섹션이 있습니다.

- 개요 섹션 - 통합 보안 관리 및 비용 최적화의 이점을 설명합니다.
- 요금 정보 - 기능 범주 및 요금 계층이 있는 확장 가능한 패널입니다.
- 요금 비교 테이블 - 기능 세부 정보와Side-by-side 비용 비교.

### 요금 비교 테이블

테이블 헤더에는 보기/편집 모드 제어와 재설정 옵션이 포함되어 있습니다. 이 표에는 비용이 두 열로 표시됩니다.

- 개별 서비스 - 별도의 보안 서비스에 대한 현재 또는 예상 비용입니다.
- Security Hub - 간소화된 요금 모델을 사용한 예상 비용입니다.

### 요금 리전

첫 번째 열에는 견적이 계산에 us-east-1 요금을 사용한다는 참고를 포함하여 요금 컨텍스트 정보가 표시됩니다. 배지는 엔터프라이즈 할인이 추정치에 포함되지 않음을 나타냅니다.

## 예상 비용 보기

비용 예측기를 사용할 때 견적을 보고, 편집하고, 재설정하고, 내보낼 수 있습니다.

기본적으로 비용 예측기는 보기 모드에서 열립니다.

예상 비용을 보려면

1. 에 설명된 방법 중 하나를 사용하여 Cost Estimator에 액세스합니다비용 예측기 액세스.
2. 요약 행의 총 월별 비용을 검토합니다.
3. 기능 그룹과 세부 비용 내역을 검토합니다.
4. 팝오버에서 설명을 보려면 기능 이름을 선택합니다.

보기 모드의 데이터 소스

예측기는 여러 소스의 데이터를 레이블로 표시합니다.

- 기본값 -의 데이터 AWS Cost Explorer (지난 30일).
- $-/mo - 비용 데이터를 사용할 수 없음(Cost Explorer 액세스를 사용할 수 없는 경우 표시됨).
- 사용자 지정 사용량 - 사용자가 입력한 값입니다.
- 활성화되지 않음 - Cost Explorer 권한이 없는 경우 표시됩니다.

## 계정별 동작

다음은 비용 예측기가 다양한 유형의 계정 및 구성에서 작동하는 방식을 설명합니다.

위임된 관리자 및 멤버 계정

교차 계정 액세스가 구성된 경우:

- Cost Explorer 데이터는 조직 전체에서 사용할 수 있습니다.
- 기본적으로 보기 모드에서 열립니다(관리 계정과 동일). 편집 모드로 전환하여 추정치를 수정할 수 있습니다.

교차 계정 액세스가 구성되지 않은 경우:

- 알림 표시: "이 계정에는 조직 사용 데이터를 사용할 수 없습니다".
- 수동 입력을 위해 기본적으로 편집 모드에서 열립니다.
- 설정 지침을 보려면 알림에서 지침 보기를 선택합니다.

관리 계정

교차 계정 역할이 생성된 경우:

- "교차 계정 액세스" 섹션에 구성된 상태가 표시됩니다.
- 확인을 위한 권장 정책을 표시합니다.
- IAM 콘솔에서 역할을 볼 수 있는 링크를 제공합니다.

교차 계정 역할이 생성되지 않은 경우:

- “교차 계정 액세스” 섹션에 설정 가이드가 표시됩니다.
- 미리 채워진 정책과 함께 step-by-step 지침을 제공합니다.
- 역할 생성을 위한 IAM 콘솔에 대한 직접 링크입니다.

역할 상태를 확인할 수 없음:

- 를 호출할 권한이 없는 경우 콘솔`iam:GetRole`은 필요한 역할을 생성했는지 확인할 수 없습니다.
- 해당 오류 메시지와 함께 “확인할 수 없음”을 표시합니다.

독립 실행형 계정

교차 계정 역할이 생성되지 않은 경우:

- 기존 동작은 변경되지 않습니다.
- Cost Explorer 데이터는 활성화되면 사용할 수 있습니다.
- 기본적으로 보기 모드에서 열립니다.

## 사용량 값 편집

편집 모드를 사용하면 차원 값을 수정하고 실시간 비용 업데이트를 볼 수 있습니다.

사용량 값을 편집하려면

1. 테이블 헤더에서 편집을 선택합니다.
2. 차원 입력 필드에 값을 입력합니다.
3. 업데이트된 비용을 자동으로 봅니다.
4. 보기를 선택하여 보기 모드로 돌아갑니다.

> **Important**
>
> - 비용 예측기 페이지에서 나가면 편집이 저장되지 않습니다.
> - 수정된 견적은 us-east-1(버지니아 북부) 요금을 사용하며 엔터프라이즈 할인은 포함하지 않습니다.
> - "현재 비용만 표시" 모드에서 편집하면 자동으로 예상 모드로 다시 전환됩니다.

## 예측기 재설정

이 작업은 모든 사용자 지정 값을 지우고 Cost Explorer에서 기본 데이터를 다시 로드합니다.

모든 값을 기본값으로 재설정하려면

1. 테이블 헤더에서 재설정을 선택합니다.
2. 확인 대화 상자에서 재설정을 선택합니다.

## 추정 내보내기

비용 예측기에서 견적 데이터를 PDF 파일로 내보낼 수 있습니다.

예상 비용을 내보내려면

1. 보기 모드에 있는지 확인합니다.
2. 페이지 헤더에서 PDF 다운로드를 선택합니다.

파일 이름이 인 PDF가 자동으로 다운로드됩니다`SecurityHub-Cost-Estimate-YYYY-MM-DD.pdf`.

## 문제 해결

이 섹션에서는 비용 예측기를 사용할 때 발생할 수 있는 일반적인 문제와 해결 방법을 다룹니다.

사용 가능한 Cost Explorer 데이터 없음

문제

알림에는 "계정에 사용할 수 있는 비용 데이터 없음"이 표시됩니다.

계정 유형별 솔루션

솔루션은 계정 유형에 따라 다릅니다.

Cost Explorer 데이터 누락에 대한 솔루션

| 계정 유형 | Solution |
| --- | --- |
| 관리 계정 | Cost Explorer를 활성화하고 데이터 처리를 위해 24시간 대기 |

| 계정 유형 | Solution |
| --- | --- |
| 위임된 관리자 | 액세스를 요청하려면 관리 계정 관리자에게 문의하세요. |
| 멤버 계정 | 액세스를 위한 연락처 관리 계정 또는 위임된 관리자 |
| 독립 실행형 계정 | Cost Explorer를 활성화하고 데이터 처리를 위해 24시간 대기 |

차선책

편집 모드에서 사용자 지정 값을 입력합니다.

교차 계정 액세스가 작동하지 않음

문제

위임된 관리자 또는 멤버 계정에는 "이 계정에 조직 사용 데이터를 사용할 수 없습니다" 알림이 표시됩니다.

다음과 같은 일반적인 원인과 해결 방법을 검토합니다.

관리 계정에 교차 계정 역할이 존재하지 않습니다.

관리 계정 관리자에게 문의하여 역할을 생성합니다. 비용 예측기는 관리 계정 사용자를 위한 안내 설정 지침을 제공합니다.

역할 이름이 정확히 일치하지 않음

필수 역할 이름: `AwsSecurityHubCostEstimatorCrossAccountRole`. IAM 콘솔의 역할 이름이 정확히 일치하는지 확인합니다(대소문자 구분).

신뢰 정책에서 계정을 허용하지 않음

신뢰 정책 보안 주체에 계정 ID와 역할 이름이 포함되어 있는지 확인합니다. 형식: `arn:aws:iam::{YOUR_ACCOUNT_ID}:role/{YOUR_ROLE_NAME}`

AssumeRole 권한 누락

IAM 보안 주체에 `sts:AssumeRole` 권한이 있는지 확인합니다. AWS 관리자에게 문의하여이 권한을 추가합니다.

해결 방법:

편집 모드에서 사용자 지정 값을 입력하여 Cost Explorer 데이터 없이 비용을 수동으로 추정합니다.

자세한 지침 받기

- 알림에서 지침 보기를 선택하여 다음을 사용하여 모달을 엽니다.
  - Step-by-step 설정 지침
  - 미리 채워진 정책 템플릿
  - 오류 관련 문제 해결 팁

권한 오류

문제

특정 API 작업에 대한 "액세스 거부" 오류입니다.

권한 오류를 해결하려면

1. 오류 메시지에서 거부된 작업을 기록해 둡니다(예: `ce:GetCostAndUsage`).
2. 복사를 선택하여 오류 세부 정보를 복사합니다.
3. 오류 세부 정보를 AWS 관리자에게 전송합니다.
4. 에 나열된 필수 IAM 권한을 요청합니다필수 IAM 권한.

> **Note**
>
> 요금 API 액세스가 거부되는 경우를 제외하고(가 모든 예상 비용을 방지함) 편집 모드를 사용하여 권한이 누락된 경우 수동 값을 입력할 수 있습니다.

기능은 "활성화되지 않음"으로 표시됩니다.

문제

기능은 "활성화되지 않음" 상태를 표시합니다.

설명

이 상태는 Cost Explorer 액세스 권한이 있지만 기능이 현재 활성화되어 있지 않은 경우에 나타납니다. 대신 $-/mo가 표시되면 계정 유형에 Cost Explorer 데이터를 사용할 수 없음을 나타냅니다.

예상 비용을 보려면

1. 편집을 선택하여 편집 모드로 전환합니다.
2. 기능의 차원 값을 입력합니다.
3. 업데이트된 예상 비용을 봅니다.

기능은 "해당 사항 없음"으로 표시됩니다.

문제

기능 개별 서비스 열에 "해당 사항 없음"이 표시됩니다.

설명

이 기능은 독립 실행형 서비스가 아닌 Security Hub 간소화된 요금을 통해서만 사용할 수 있습니다.

수정된 비용이 Cost Explorer와 일치하지 않음

문제

편집된 비용은 원래 Cost Explorer 값과 다릅니다.

설명

수정된 견적은 us-east-1(버지니아 북부) 요금 요금을 사용하며 엔터프라이즈 할인은 포함하지 않습니다. Cost Explorer 데이터는 적용 가능한 할인과 함께 실제 비용을 반영합니다.

## 중요 정보

- 예측은 관찰된 사용량과 사용자 제공 사용량 및 공개 요금 정보를 기반으로 합니다. 실제 비용은 사용량 패턴 및 엔터프라이즈 계약에 따라 다를 수 있습니다.
- 30일 룩백 - Cost Explorer 데이터는 지난 30일 사용량을 반영합니다.
- 요금 리전 - 모든 견적은 us-east-1(버지니아 북부) 요금을 사용합니다.
- 설정에 영향 없음 - 예측기의 변경 사항은 현재 Security Hub 또는 서비스 구성에 영향을 주지 않습니다.
- 엔터프라이즈 할인 - 수정된 견적에는 엔터프라이즈 할인이 포함되지 않습니다. Cost Explorer 데이터에만 실제 할인 비용이 반영됩니다.

- 데이터 새로 고침 - Cost Explorer 데이터가 매일 업데이트됩니다. 페이지를 새로 고쳐 최신 데이터를 확인합니다.

### 관련 정보

- AWS Security Hub 요금
- AWS Cost Explorer 사용 설명서
- AWS 요금 API 참조
- Security Hub 활성화

## Security Hub 활성화

모든 AWS 계정에 대해 Security Hub를 활성화할 수 있습니다. 설명서의이 섹션에서는 AWS 조직 또는 독립 실행형 계정에 대해 Security Hub를 활성화하는 데 필요한 모든 단계를 설명합니다.

Security Hub를 활성화하는 방법에 대한 간략한 데모를 보려면 Security Hub 온보딩 연습 및 데모 동영상을 시청하세요.

### AWS 조직에 대한 Security Hub 활성화

이 섹션에는 다음 세 단계가 포함되어 있습니다.

- 1단계에서 AWS 조직 관리 계정은 AWS 조직의 위임된 관리자를 지정하고, 위임된 관리자 정책을 생성하고, 선택적으로 자신의 계정에 대해 Security Hub를 활성화합니다.
- 2단계에서 조직의 위임된 관리자는 자신의 계정에 대해 Security Hub를 활성화합니다.
- 3단계에서 조직의 위임된 관리자는 Security Hub 및 기타 지원되는 보안 서비스에 대해 조직의 모든 멤버 계정을 구성합니다.

## 1단계. 관리자 계정 위임 및 선택적으로 AWS 조직 관리 계정에서 Security Hub 활성화

> **Note**
>
> 조직 관리 계정의 한 리전에서이 단계를 완료합니다.

Security Hub에 위임된 관리자 계정을 할당할 때 위임된 관리자에 대해 선택할 수 있는 계정은 Security Hub CSPM에 대해 위임된 관리자를 구성한 방법에 따라 달라집니다. Security Hub CSPM에 대해 위임된 관리자를 구성했고 해당 계정이 조직 관리 계정이 아닌 경우 해당 계정은 Security Hub 위임된 관리자로 자동으로 설정되며 다른 계정을 선택할 수 없습니다. Security Hub CSPM의 위임된 관리자 계정이 조직 관리 계정으로 설정되거나 전혀 설정되지 않은 경우 조직 관리 계정을 제외하고 Security Hub 위임된 관리자 계정으로 할당할 계정을 선택할 수 있습니다.

Security Hub에서 위임된 관리자를 지정하는 방법에 대한 자세한 내용은 Security Hub에서 위임된 관리자 계정 지정을 참조하세요. Security Hub에서 위임된 관리자 정책을 생성하는 방법에 대한 자세한 내용은 Security Hub에서 위임된 관리자 정책 생성을 참조하세요.

Security Hub의 관리자를 지정하려면

1. AWS 조직 관리 AWS 계정 자격 증명으로 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. Security Hub 홈페이지에서 Security Hub를 선택한 다음 시작하기를 선택합니다.
3. 위임된 관리자 섹션에서 제공된 옵션에 따라 관리자 계정을 선택합니다. 일관된 거버넌스를 위해 보안 서비스 전반에 걸쳐 동일한 위임된 관리자를 사용하는 것이 가장 좋습니다.
4. 신뢰할 수 있는 액세스 확인란을 선택합니다. 이 옵션을 선택하면 위임된 관리자 계정에 멤버 계정에서 GuardDuty 맬웨어 보호와 같은 특정 기능을 구성할 수 있는 기능이 부여됩니다. 이 옵션을 선택 취소하면 Security Hub는 사용자를 대신하여 이러한 기능을 활성화할 수 없으며 해당 기능이 연결된 서비스를 통해 직접 활성화해야 합니다.
5. (선택 사항) 계정 활성화에서 확인란을 선택하여 AWS 계정에 대해 Security Hub를 활성화합니다.

6. 위임된 관리자 정책에서 다음 옵션 중 하나를 선택하여 정책 설명을 추가합니다.

   a. (옵션 1) 업데이트하기를 선택합니다. 정책 설명 아래의 상자를 선택하여 Security Hub가 위임된 관리자에게 필요한 모든 권한을 부여하는 위임 정책을 자동으로 생성하는지 확인합니다.

   b. (옵션 2) 수동으로 연결하기를 선택합니다. 복사 및 연결을 선택합니다. AWS Organizations 콘솔의 위임된 관리자 AWS Organizations에서 위임을 선택하고 위임 정책 편집기에 리소스 정책을 붙여 넣습니다. 정책 생성을 선택하세요. Security Hub 콘솔에서 현재 위치의 탭을 엽니다.

7. 구성을 선택합니다.

## 2단계. 위임된 관리자 계정에서 Security Hub 활성화

위임된 관리자 계정이이 단계를 완료합니다. AWS 조직 관리 계정이 조직의 위임된 관리자를 지정한 후 위임된 관리자는 전체 AWS 조직에 대해를 활성화하기 전에 자신의 계정에 대해 Security Hub를 활성화해야 합니다.

위임된 관리자 계정에서 Security Hub를 활성화하려면

1. 위임된 관리자 자격 증명으로 AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. Security Hub 홈페이지에서 시작하기를 선택합니다.
3. 보안 기능 섹션에서는 Security Hub의 기본 리소스당 가격에 자동으로 활성화되고 포함되는 기능을 간략하게 설명합니다.
4. (선택 사항) 태그에서 계정 설정에 키-값 페어를 추가할지 여부를 결정합니다.
5. Security Hub 활성화를 선택하여 Security Hub 활성화를 완료합니다.
6. (권장) 팝업에서 내 조직 구성을 선택하고 3단계로 진행합니다.

## 3단계. 모든 멤버 계정에서 Security Hub를 활성화하는 정책 생성

조직의 위임된 관리자 계정에서 Security Hub를 활성화한 후에는 조직 멤버 계정에서 활성화할 서비스와 기능을 정의하는 정책을 생성해야 합니다. 자세한 내용은 정책 유형으로 구성 활성화를 참조하세요.

Security Hub를 활성화하면 계정에 다음 리소스가 생성됩니다.

- AWSServiceRoleForSecurityHubV2라는 서비스 연결 역할입니다.
- 서비스 연결 구성 레코더. 자세한 내용은 Security Hub 개념 설명서의 서비스 연결 레코더를 참조하세요.

- 서비스 연결 분석기입니다. 자세한 내용은 Security Hub 개념 설명서의 서비스 연결 분석기를 참조하세요.

## 독립형 계정에서 Security Hub 활성화

이 절차에서는 독립형 계정에서 Security Hub를 활성화하는 방법을 설명합니다. 독립 실행형 계정은 AWS 조직을 활성화하지 AWS 계정 않은 입니다.

독립형 계정에서 Security Hub를 활성화하려면

1. AWS 계정 자격 증명으로 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. Security Hub 홈페이지에서 시작하기를 선택합니다.
3. 보안 기능 섹션에서 다음 중 하나를 수행합니다.
   a. (옵션 1) 모든 기능 활성화를 선택합니다. 이렇게 하면 모든 Security Hub 필수 기능, 위협 분석 및 추가 기능이 활성화됩니다.
   b. (옵션 2) 기능 사용자 지정을 선택합니다. 보안 관리, 위협 분석 및 취약성 관리 섹션에서 활성화할 기능을 선택합니다. Security Hub 필수 계획 기능의 일부인 기능은 선택 취소할 수 없습니다.
4. 리전 섹션에서 모든 리전 활성화 또는 특정 리전 활성화를 선택합니다. 모든 리전 활성화를 선택하는 경우 새 리전을 자동으로 활성화할지 여부를 결정할 수 있습니다. 특정 리전 활성화를 선택하는 경우 활성화할 리전을 선택해야 합니다.
5. (선택 사항) 리소스 태그의 경우 구성을 쉽게 식별할 수 있도록 태그를 키-값 페어로 추가합니다.
6. Security Hub 활성화를 선택합니다.

Security Hub를 활성화하면 서비스를 활성화한 각 계정에 다음 리소스가 생성됩니다.

- AWSServiceRoleForSecurityHubV2라는 서비스 연결 역할입니다.
- 서비스 연결 구성 레코더. 자세한 내용은 Security Hub 개념 설명서의 서비스 연결 레코더를 참조하세요.
- 서비스 연결 분석기입니다. 자세한 내용은 Security Hub 개념 설명서의 서비스 연결 분석기를 참조하세요.

# Security Hub에서 위임된 관리자 지정

AWS 조직 관리 계정에서 조직의 위임된 관리자를 지정할 수 있습니다. 일관된 거버넌스를 위해 보안 서비스 전반에 걸쳐 동일한 위임된 관리자를 사용하는 것이 가장 좋습니다.

이 주제의 절차에서는 Security Hub에서 위임된 관리자를 지정하는 방법을 설명합니다. 여기서는 이전에 Security Hub를 활성화했지만 활성화 워크플로 중에 위임된 관리자를 지정하지 않았다고 가정합니다.

고려 사항

Security Hub에서 위임된 관리자를 지정할 때는 다음 사항을 고려해야 합니다.

- AWS 조직 관리 계정은 Security Hub CSPM에서 자신을 위임된 관리자로 지정할 수 있지만 Security Hub에서 자신을 위임된 관리자로 지정할 수는 없습니다. 이 시나리오에서 관리 계정은 Security Hub에서 다른를 위임된 관리자 AWS 계정 로 지정해야 합니다.
- AWS 조직 관리 계정이 Security Hub CSPM에서 위임된 관리자를 지정하면 해당 위임된 관리자가 자동으로 Security Hub의 위임된 관리자가 됩니다. 이 시나리오에서 Security Hub는이 특정 만 위임된 관리자 역할을 AWS 계정 하도록 허용합니다.

> **Note**
>
> Security Hub CSPM 콘솔, Security Hub 콘솔 또는 AWS Organizations API를 통해 위임된 관리자를 제거하면 두 서비스에서 모두 제거됩니다. Security Hub CSPM에서 위임된 관리자가 제거되면 중앙 구성이 자동으로 옵트아웃합니다.

## Security Hub 활성화 후 위임된 관리자 지정

이 절차는 AWS 조직 관리 계정이 완료해야 하는 절차입니다. 조직 AWS 관리 계정이 이전에 Security Hub를 활성화했지만 활성화 워크플로 중에 위임된 관리자를 지정하지 않았다고 가정합니다.

> **Note**
>
> 이 절차를 완료한 후에는 조직의 위임된 관리자가 Security Hub를 구성하고 AWS Organizations에서 특정 작업을 수행하도록 허용하는 정책을 생성해야 합니다. 자세한 내용은 Security Hub에서 위임된 관리자 정책 생성을 참조하세요.

Security Hub에서 위임된 관리자를 지정하려면

1. 조직 관리 AWS 계정 자격 증명으로 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 일반을 선택합니다.
3. 위임된 관리자에서 구성을 선택합니다. 제공된 중 하나를 선택하거나 조직의 위임된 관리자로 지정 AWS 계정 하려는의 12자리 AWS 계정 숫자를 AWS 계정입력합니다. 저장을 선택합니다.

## Security Hub에서 위임된 관리자 정책 생성

AWS 조직 관리 계정은 위임된 관리자가 Security Hub를 구성하고에서 특정 작업을 수행하도록 허용하는 정책을 생성할 수 있습니다 AWS Organizations. 이 주제의 절차에서는 해당 정책을 생성하는 방법을 설명합니다. 절차를 완료할 때 Security Hub에서 정책을 생성하도록 허용하거나 수동으로 정책을 생성할 수 있습니다. 특정 사용 사례에 맞게 사용자 지정하려는 경우가 아니면 Security Hub에서 정책을 생성하도록 허용합니다.

조직 관리 계정이 Security Hub를 활성화하고 위임된 관리자를 지정했지만 활성화 워크플로 중에 정책 생성을 건너뛴 경우에만이 절차를 완료하세요. 이 정책을 업데이트하는 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AWS Organizations를 사용하여 리소스 기반 위임 정책 업데이트를 참조하세요.

> **Note**
>
> 이 절차를 완료한 후 위임된 관리자는 조직의 멤버 계정을 관리하는 정책을 생성할 수 있습니다. 자세한 내용은 위임된 관리자로 멤버 계정을 관리하기 위한 정책 생성을 참조하세요.

위임된 관리자 정책을 생성하려면

1. 조직 관리 AWS 계정 자격 증명으로 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 일반을 선택합니다.
3. 위임된 관리자 정책에서 다음 중 하나를 수행합니다.
   - 정책 생성을 선택합니다. 정책 설명 아래의 상자를 선택하여 Security Hub가 위임된 관리자에게 필요한 모든 권한을 부여하는 위임 정책을 자동으로 생성하는지 확인합니다.

- 정책을 엽니다. 복사 및 연결을 선택합니다. AWS Organizations 콘솔의 위임된 관리자 AWS Organizations에서 위임을 선택하고 위임 정책 편집기에 리소스 정책을 붙여 넣습니다. 정책 생성을 선택하세요. Security Hub 콘솔에서 현재 위치의 탭을 열고 구성을 선택합니다.

# AWS 조직 내 멤버 계정 구성 관리

AWS 조직의 위임된 관리자는 멤버 계정 및 리전에서 보안 기능을 구성할 수 있습니다. 정책 및 배포라는 두 가지 유형의 구성을 사용할 수 있습니다. 정책은 AWS Security Hub 및 Amazon Inspector의 계정 및 리전에 대한 AWS Organizations 정책을 생성합니다. 배포는 Amazon GuardDuty 및 AWS Security Hub CSPM에 대해 선택한 계정 및 리전에서 보안 기능을 활성화하는 일회성 작업입니다. 정책과 달리 배포를 보거나 편집할 수 없으며 배포는 새로 활성화된 계정에 적용되지 않습니다. 또는 Amazon GuardDuty 및 AWS Security Hub CSPM에서 새 멤버 계정에 대한 자동 활성화 기능을 사용할 수 있습니다.

## Security Hub 구성 카탈로그

Security Hub의 구성 카탈로그는 Security Hub에서 제공하는 보안 기능에 대해 AWS 조직 계정을 구성하는 데 도움이 되는 여러 옵션을 제공합니다.

다음은 Security Hub 구성 카탈로그에서 사용할 수 있는 옵션입니다.

Security Hub(필수 및 추가 기능)

이는 Security Hub에 배포하기 위한 권장 구성입니다.

유형: 정책 및 배포

설명:이 구성은 Security Hub의 필수 보안 관리, 태세 관리, 위협 분석 및 취약성 관리 기능을 활성화합니다. 선택적으로 추가 기능을 활성화합니다.

GuardDuty의 위협 분석

유형: 배포

설명: 선택한 Amazon GuardDuty 기능을 켜서 AWS 환경의 AWS 데이터 소스 및 로그를 지속적으로 모니터링, 분석 및 처리합니다.

AWS Security Hub CSPM의 태세 관리

유형: 배포

설명:이 구성은 AWS 계정 및 리소스가 보안 모범 사례에서 벗어나는 시점을 감지하는 Security Hub CSPM의 표준 및 제어를 활성화합니다.

Amazon Inspector의 취약성 관리

유형: 정책

설명:이 구성은 워크로드, 인스턴스, 컨테이너 이미지 및 기타 리소스를 자동으로 검색하고 취약성 및 네트워크 노출을 스캔하는 선택한 Amazon Inspector 기능을 활성화합니다.

## 정책 유형으로 구성 활성화

다음 절차에서는 AWS 조직 계정에 대한 정책 유형으로 구성을 생성하는 방법을 설명합니다. 구성 정책을 생성하려면 먼저 AWS 조직 관리 계정에서 위임된 관리자 정책을 생성해야 합니다. Security Hub에서 위임된 관리자 정책을 생성하는 방법에 대한 자세한 내용은 Security Hub에서 위임된 관리자 정책 생성을 참조하세요.

멤버 계정을 활성화 및 비활성화하는 정책을 생성하려면

1. 위임된 관리자 자격 증명으로 AWS 계정을 사용하여 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 구성을 선택합니다.
3. 구성 카탈로그에서 정책 또는 정책 및 배포 유형이 있는 항목을 선택합니다. Security Hub를 완전히 구성하려면 Security Hub(필수 및 추가 기능)를 선택합니다.
4. Security Hub 구성 페이지의 세부 정보 섹션에 정책의 이름과 설명을 입력합니다.
5. 보안 기능 섹션에서 다음 중 하나를 선택합니다.
   - 모든 기능 활성화 - 모든 Security Hub 필수 기능, 위협 분석 및 추가 기능을 켭니다.
   - 기능 사용자 지정 - 보안 관리, 위협 분석 및 취약성 관리 섹션에서 기능을 선택합니다. Security Hub 필수 계획의 일부인 기능은 선택 취소할 수 없습니다.
6. 계정 선택 섹션에서 다음 옵션 중 하나를 선택합니다.
   - 모든 조직 단위 및 계정 - 전체 조직에 구성을 적용합니다.
   - 특정 조직 단위 및 계정 - 검색 창 또는 조직 구조 트리를 사용하여 정책이 적용되는 조직 단위 및 계정을 선택합니다.
   - 조직 단위 또는 계정 없음 - 조직 단위 또는 계정에 구성을 적용하지 않습니다.
7. 리전 섹션에서 다음 중 하나를 선택합니다.
   - 모든 리전 활성화 - 선택적으로 새 리전을 자동으로 활성화할지 여부를 선택합니다.

- 모든 리전 비활성화 - 선택적으로 새 리전을 자동으로 비활성화할지 여부를 선택합니다.
- 리전 지정 - 활성화 및 비활성화할 리전을 선택합니다.

8. (선택 사항) 고급 설정은 AWS Organizations 사용 설명서의 상속 연산자를 참조하세요.
9. (선택 사항) 리소스 태그의 경우 구성을 식별하는 데 도움이 되도록 태그를 키-값 페어로 추가합니다.
10. 다음을 선택합니다.
11. 변경 내용을 검토하고 적용을 선택합니다.

    정책의 구성 상태가 정책 페이지 상단에 표시됩니다. 각 기능은 성공적으로 구성되었는지 또는 배포 실패가 있는지를 나타내는 상태를 제공합니다. 실패의 경우 실패 링크를 선택하여 자세한 내용을 확인합니다. 계정 수준에서 유효 정책을 보려면 구성 페이지에서 조직 탭을 검토하세요.

## 배포 유형으로 구성 활성화

다음 절차에서는 AWS 조직 계정에 대한 배포 유형으로 구성을 생성하는 방법을 설명합니다.

멤버 계정을 활성화하는 배포를 생성하려면

1. 위임된 관리자 자격 증명으로 AWS 계정을 사용하여 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 구성을 선택합니다.
3. 구성 카탈로그에서 배포 유형이 있는 항목을 선택합니다.
4. 보안 기능 섹션에서 활성화할 보안 기능을 선택합니다.
5. 계정 선택 섹션에서 다음 옵션 중 하나를 선택합니다.

    - 모든 조직 단위 및 계정 - 전체 조직에 배포를 적용합니다.
    - 특정 조직 단위 및 계정 - 검색 창 또는 조직 구조 트리를 사용하여 배포가 적용되는 조직 단위 및 계정을 선택합니다.
    - 조직 단위 또는 계정 없음 - 조직 단위 또는 계정에 배포를 적용하지 않습니다.

6. 리전 섹션에서 다음 중 하나를 선택합니다.

    - 모든 리전 활성화 - 선택적으로 새 리전을 자동으로 활성화할지 여부를 선택합니다.
    - 모든 리전 비활성화 - 선택적으로 새 리전을 자동으로 비활성화할지 여부를 선택합니다.
    - 리전 지정 - 활성화 및 비활성화할 리전을 선택합니다.

7. 구성을 선택합니다.

## 구성 정책 편집

구성 정책과 연결된 기능, 리전 및 계정을 편집할 수 있습니다. 편집할 정책을 열면 콘솔에 현재 구성이 표시됩니다.

> **Note**
>
> 변경 사항은 업데이트된 정책에서 선택한 기능에만 적용됩니다. 선택하지 않은 기능은 정책의 계정 및 리전에 걸쳐 기존 구성을 유지합니다.

구성 정책을 편집하려면

1. 위임된 관리자 자격 증명으로 AWS 계정을 사용하여 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 구성을 선택합니다.
3. 구성된 정책 탭에서 편집하려는 정책의 라디오 버튼을 선택한 다음 편집을 선택합니다.
4. 기능 섹션에서 다음 중 하나를 선택합니다.
   - 모든 기능 구성 및 활성화 - 정책의 모든 기능을 활성화합니다.
   - 개별 기능을 선택하고 각 기능에 대해 활성화, 비활성화 또는 사용자 지정을 선택합니다.
5. 계정 선택 섹션에서 다음 옵션 중 하나를 선택합니다.
   - 모든 조직 단위 및 계정 - 전체 조직에 정책을 적용합니다.
   - 특정 조직 단위 및 계정 - 검색 창 또는 조직 구조 트리를 사용하여 정책이 적용되는 조직 단위 및 계정을 선택합니다.
   - 조직 단위 또는 계정 없음 - 모든 대상에서 정책을 제거합니다.
6. 리전 섹션에서 정책이 적용되는 리전을 구성합니다. 옵션은 기능 선택에 따라 다릅니다.

   모든 기능을 활성화하도록 선택한 경우:

   - 선택한 모든 기능에서 - 모든 기능에 대해 동일한 리전 구성을 설정합니다.
   - 기능별 - 각 기능에 대해 개별적으로 리전을 선택할 수 있습니다.

   그런 다음 모든 리전 활성화(새 리전을 자동으로 활성화하는 옵션 사용) 또는 일부 리전에서 활성화를 선택하여 특정 리전을 선택합니다.

개별 기능에 대해 혼합 작업(활성화, 비활성화 또는 사용자 지정)을 선택한 경우:

- 선택한 모든 기능이 동일한 작업을 공유하는 경우 선택한 모든 기능에서를 선택하여 리전을 균일하게 설정합니다. 각 기능에 대해 리전을 개별적으로 설정하려면 기능별을 선택합니다.
- 기능에 다른 작업이 있는 경우 각 기능에 리전을 개별적으로 할당해야 합니다.
- 사용자 지정 작업이 있는 기능의 경우 선택한 모든 기능에서를 선택하여 모든 기능에 대해 리전을 균일하게 설정합니다. 각 기능에 대해 리전을 개별적으로 구성하려면 기능별을 선택합니다.

7. 다음을 선택합니다.
8. 변경 사항을 검토한 다음 업데이트를 선택합니다. 업데이트된 정책은 대상 계정을 구성합니다.

### 구성 정책 삭제

구성 정책을 삭제할 수 있습니다. 정책을 삭제하면 서비스는 연결된 모든 계정과 조직 단위를 정책에서 제거합니다.

구성 정책 삭제

1. 위임된 관리자 자격 증명으로 AWS 계정을 사용하여 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 구성을 선택합니다.
3. 구성된 정책 탭에서 삭제할 정책을 선택한 다음 삭제를 선택합니다.
4. 확인 상자에 `delete`를 입력한 다음 삭제를 선택합니다.

## Security Hub에서 위임된 관리자 계정 제거

언제든지 Security Hub 콘솔에서 위임된 관리자 계정을 제거할 수 있습니다. 그러나이 작업은 Security Hub와 Security Hub CSPM 모두에서 위임된 관리자를 제거합니다. 보안 계정으로 이 작업을 확인한 경우에만 이 작업을 수행하는 것이 좋습니다.

> **Note**
>
> 조직 관리 계정 이외의 계정을 Security Hub CSPM 위임된 관리자로 사용하는 경우 Security Hub CSPM 콘솔 또는 AWS Organizations API를 통해 제거하면 Security Hub에서도 제거됩니다.

마찬가지로 Security Hub 콘솔 또는 AWS Organizations API를 통해 Security Hub 위임된 관리자를 제거하면 Security Hub CSPM에서도 제거됩니다. Security Hub CSPM에서 위임된 관리자가 제거되면 중앙 구성이 자동으로 옵트아웃합니다.

위임된 관리자 계정을 제거하려면

1. 조직 관리 AWS 계정 자격 증명으로 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 일반을 선택합니다.
3. 위임된 관리자에서 위임된 관리자 제거를 선택합니다. 확인 대화 상자에서 제거를 입력하고 제거를 선택합니다.

## Security Hub 다시 활성화

Security Hub 정책을 사용하여 이전에 비활성화된 계정에서 Security Hub를 다시 활성화하기 전에 먼저 비활성화 정책을 분리해야 합니다. 비활성화 정책이 계정 또는 조직 단위에 연결된 상태에서 Security Hub를 다시 활성화하려고 하면 비활성화 정책이 활성화를 재정의하고 Security Hub는 비활성화된 상태로 유지됩니다.

조직 또는 계정에 대한 Security Hub 비활성화 정책을 제거하려면

1. 조직 관리 AWS 계정 자격 증명으로 계정을 사용하여 로그인합니다. https://console.aws.amazon.com/organizations/v2/home AWS Organizations 콘솔을 엽니다.
2. 탐색 패널에서 AWS 계정을 선택합니다.
3. 현재 Security Hub 비활성화 정책이 전체 조직에 대한 것인 경우 조직 구조에서 루트를 선택합니다. 현재 Security Hub 비활성화 정책이 특정 계정에 대한 정책인 경우 조직 구조에서 특정 계정을 선택한 다음 각 계정에 대한 나머지 단계를 따릅니다.
4. 정책 탭에서 Security Hub 정책이라는 제목의 섹션을 찾습니다.
5. Security Hub를 비활성화하는 정책 옆의 라디오 버튼을 선택합니다. 분리를 선택합니다.

조직 또는 계정에서 정책을 분리한 후 Security Hub를 다시 활성화할 수 있습니다. Security Hub를 다시 활성화하는 방법에 대한 자세한 내용은 AWS Organization에서 멤버 계정의 구성 관리를 참조하세요.

# Security Hub 권장 사항

의 다음 보안 서비스는 결과를 OCSF 형식으로 Security Hub에 AWS 전송합니다. Security Hub를 활성화한 후 추가 보안을 AWS 서비스 위해 이를 활성화합니다.

Security Hub CSPM

Security Hub CSPM을 활성화하면 AWS에서의 보안 상태를 포괄적으로 파악할 수 있습니다. 이를 통해 고객 환경에서 보안 업계 표준 및 모범 사례를 준수하는지 평가할 수도 있습니다. Security Hub CSPM을 활성화하지 않고 Security Hub를 시작할 수 있지만 Security Hub CSPM을 활성화하면 Security Hub가 Security Hub CSPM의 보안 신호를 상호 연관시켜 태세 관리를 개선할 수 있습니다.

Security Hub CSPM을 활성화하는 경우 계정에 대한 AWS 기본 보안 모범 사례 표준도 활성화하는 것이 좋습니다. 이 표준은 AWS 계정 및 리소스가 보안 모범 사례에서 벗어나는 시점을 감지하는 제어 세트로 구성됩니다. 계정에 AWS 대한 기본 보안 모범 사례 표준을 활성화하면 AWS Security Hub CSPM은 다음 리소스 유형에 대한 제어를 포함하여 모든 제어를 자동으로 활성화합니다.

- 계정 제어
- Amazon DynamoDB 제어
- Amazon Elastic Compute Cloud 제어
- AWS Identity and Access Management (IAM) 제어
- AWS Lambda 제어
- Amazon Relational Database Service(Amazon RDS) 콘솔
- Amazon Simple Storage Service 제어

이 목록의 모든 제어를 비활성화할 수 있습니다. 그러나 이러한 제어를 비활성화하면 지원되는 리소스에 대한 조사 노출 결과를 수신할 수 없습니다. AWS 기본 보안 모범 사례 표준에 적용되는 제어에 대한 자세한 내용은 AWS 기본 보안 모범 사례 v1.0.0(FSBP) 표준을 참조하세요.

GuardDuty

GuardDuty를 활성화하면 Security Hub 콘솔의 대시보드에서 모든 위협 및 보안 적용 범위 조사 결과를 볼 수 있습니다. GuardDuty를 활성화하면 GuardDuty는 Security Hub로 데이터(OCSF 형식)를 자동으로 전송하기 시작합니다.

Amazon Inspector –

Amazon Inspector를 활성화하면 Security Hub 콘솔의 대시보드에서 모든 노출 및 보안 적용 범위 조사 결과를 볼 수 있습니다. Amazon Inspector를 활성화하면 Amazon Inspector는 Security Hub로 데이터(OCSF 형식)를 자동으로 전송하기 시작합니다.

Amazon EC2 스캔 및 Lambda 표준 스캔을 활성화하는 것이 좋습니다. Amazon EC2 스캔을 활성화하면 Amazon Inspector가 계정의 Amazon EC2 인스턴스에 패키지 취약성 및 네트워크 연결성 문제가 있는지 검사합니다. Lambda 표준 스캔을 활성화하면 Amazon Inspector가 Lambda 함수에서 패키지 종속성의 소프트웨어 취약성을 스캔합니다. 자세한 내용은 Amazon Inspector 사용 설명서의 스캔 유형 활성화를 참조하세요.

Macie

Macie를 활성화하면 Amazon S3 버킷에 대한 추가 노출을 탐지할 수 있습니다. Macie가 매일 Amazon S3 버킷 인벤토리를 평가할 수 있도록 민감한 데이터 자동 검색을 구성하는 것이 좋습니다.

# Security Hub의 계정 적용 범위

계정 적용 범위 페이지에는 Security Hub와 통합 보안 기능이 활성화된 조직의 계정 및 리전이 표시됩니다. 이러한 기능에는 Amazon Inspector, Amazon GuardDuty, AWS Security Hub CSPM, Amazon Macie와 같은 서비스가 포함됩니다. 이 페이지를 사용하여 적용 범위 격차를 식별하고 조직 전체의 기능 채택을 추적할 수 있습니다.

## 계정 적용 범위 페이지

계정 적용 범위 페이지에서 집계된 적용 범위 지표를 볼 수 있습니다. 계정 수준 세부 정보는 계정 탭을 사용하고 특정 적용 범위 격차를 검토하려면 적용 범위 결과 탭을 사용합니다.

Security Hub 계정 적용 범위 페이지에 액세스하려면

1. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 설정에서 계정 적용 범위를 선택합니다.

### 개요 섹션

개요 섹션에는 모니터링되는 모든 계정의 집계된 보안 적용 범위 지표가 표시됩니다. 위임된 관리자 계정의 경우이 섹션에는 조직 전체의 Security Hub 활성화 세부 정보가 표시되어 모든 멤버 계정의 적용 범위에 대한 가시성을 제공합니다. 이 상위 수준 시각화는 Security Hub 및 각 보안 기능이 활성화된 계정의 비율을 보여 주며, 보안 태세에 대한 포괄적인 보기를 제공합니다. Security Hub 적용 범위의 백분

율을 선택하여 리전별로 활성화된 계정의 분석을 볼 수 있습니다. 각 기능 백분율을 선택하여 해당 기능별로 적용 범위 조사 결과를 필터링할 수 있습니다.

개요 섹션의 백분율은 다음 계산을 사용하여 결정됩니다.

- Security Hub 활성화 = (Security Hub가 활성화된 계정 및 리전 페어 수) ÷ (조직의 총 계정 × Security Hub를 사용할 수 있는 리전)
- 서비스 적용 범위 = (기능이 활성화된 활성화된 계정 및 구성된 리전 페어 수) ÷ (계정이 활성화되고 기능을 사용할 수 있는 구성된 리전에서 활성화된 계정 및 구성된 리전 페어의 총 수)

> **구성된 리전**
>
> 홈 리전 설정의 경우 구성된 리전에는 홈 리전과 연결된 리전이 포함됩니다. 다른 모든 설정의 경우 구성된 리전은 현재 리전만 참조합니다.

## 계정 탭

이 탭은 Security Hub 위임된 관리자 계정에서만 사용할 수 있습니다. 계정 탭을 사용하여 계정별 적용 범위를 분석합니다. Security Hub 열에는 각 계정에 대해 Security Hub가 활성화된 리전 수가 표시됩니다. 옵트인 리전(기본적으로 비활성화된 리전)에서 탭을 볼 때는이 열이 표시되지 않습니다. 각 보안 기능은 선택 시 개별 기능의 세부 분석과 해당 기능 내의 적용 범위 백분율을 표시하는 적용 범위 백분율을 표시합니다. 이러한 백분율을 선택하면 Security Hub는 결과를 필터링하여 해당 기능 및 계정에 대한 적용 범위를 표시합니다.

계정 탭의 백분율은 다음 계산을 사용하여 결정됩니다.

계정 탭 적용 범위 = (기능이 활성화된 리전 수) ÷ (기능을 사용할 수 있는 리전)

적용 범위 백분율이 0%로 표시될 수 있는 몇 가지 경우가 있습니다.

- Security Hub는 계정에서 활성화되지 않으므로 적용 범위 조사 결과를 수집하지 않습니다.
- Security Hub는 적용 범위 조사 결과가 생성될 때까지 기다리고 있습니다.

## 적용 범위 조사 결과 탭

적용 범위 조사 결과 탭에는 계정 및 리전에서 활성화 또는 비활성화된 보안 기능에 대한 정보 조사 결과가 나열됩니다. 이러한 결과는 보안 적용 범위를 강화할 수 있는 영역을 식별하는 데 도움이 됩니다. 각 결과에는 결과 제목, 영향을 받는 계정 및 리전, 현재 상태가 표시됩니다. 또한 각 결과에는 해당 기

능에 대한 구성을 관리할 수 있는 개별 서비스 또는 보안 서비스에 대한 구성을 업데이트할 수 있는 Security Hub 구성 페이지로 연결되는 구성 링크가 있습니다.

계정-리전 조합에 해당 보안 기능을 적용할 수 없는 경우 적용 범위 없음 상태의 적용 범위 조사 결과를 억제할 수 있습니다. Security Hub는 보안 적용 범위 백분율 계산에서 억제된 조사 결과를 제외합니다.

적용 범위 조사 결과와 이를 억제하는 방법에 대한 자세한 내용은 Security Hub의 적용 범위 조사 결과를 참조하세요.

## 보안 적용 범위 위젯

계정 적용 범위는 Security Hub 요약 대시보드의 보안 적용 범위 위젯을 통해 볼 수도 있습니다. 자세한 내용은 보안 적용 범위 위젯을 참조하세요.

# Security Hub 확장 계획

Security Hub 확장 계획을 사용하면 클라우드, 엔드포인트, 네트워크, 자격 증명, 데이터, 이메일 및 브라우저에서 전체 엔터프라이즈 자산을 보호할 수 있습니다. AWS Security Hub를 통합 보안 운영 경험의 중심으로 사용합니다. Security Hub 확장 플랜을 사용하면 선결제 투자나 장기 약정 없이 보안 요구 사항을 해결하는 파트너 솔루션을 선택하고 유연한 pay-as-you-go제 요금에 가입할 수 있습니다. 비즈니스 요구 사항이 발전함에 따라 파트너 솔루션을 추가하거나 제거할 수 있습니다.

Security Hub 확장 플랜은 Security Hub Essentials 플랜을 활성화한 모든 고객이 사용할 수 있습니다. Security Hub 확장 요금제에 대한 요금은를 레코드 판매자 AWS 로 사용하여 월별 AWS 청구서에 표시됩니다.

모든 솔루션에 대한 Security Hub 확장 플랜 요금은 Security Hub 요금 세부 정보 페이지의 확장 플랜 탭에서 확인할 수 있습니다.

## Security Hub 확장 계획에 대한 권한

Security Hub 확장 계획에서 파트너 제품을 구독하려면 Security Hub 권한 외에도 다음 권한이 필요합니다.

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

Security Hub 확장 계획에서 파트너 제품의 구독을 취소하려면 Security Hub 권한 외에도 다음 권한이 필요합니다.

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

AWS Marketplace 권한에 대한 자세한 내용은 AWS Marketplace 구매자 안내서의 Marketplace 구독에 대한 액세스 제어를 참조하세요. AWS

## 확장 플랜 파트너 검토 및 가입

Security Hub 확장 계획은 Security Hub 위임된 관리자 계정 또는 독립 실행형 계정을 통해 액세스할 수 있습니다. Security Hub 확장 계획 페이지에서는 각 파트너에 대한 세부 정보를 보고, 파트너 솔루션에 대한 구독을 시작하고, 파트너의 온보딩 페이지를 통해 각 파트너의 솔루션에 대한 온보딩 프로세스를 시작할 수 있습니다.

Security Hub 확장 계획에 액세스하고 파트너의 제품에 가입하려면

1. 위임된 관리자 또는 독립 실행형 계정 자격 증명을 사용하여 AWS Management Console에 로그인합니다.
2. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
3. 탐색 창에서 관리를 선택한 다음 확장 계획을 선택합니다.
4. 가입하려는 각 파트너 솔루션에 대해 제품 보기를 선택합니다.
5. 제품 요금 세부 정보를 검토한 다음 파트너 제품에 대한 온보딩 프로세스를 시작할 준비가 되면 구독을 선택합니다.
6. 구독 프로세스가 완료되면 파트너의 가입 페이지로 리디렉션되도록 계정 설정을 선택합니다.
7. 파트너 가입 페이지에 필요한 정보를 제공하고 파트너가 제공하는 다음 단계에 따라 온보딩 단계를 완료합니다.

> **Important**
>
> 파트너 제품에 대한 온보딩 프로세스를 완료할 때까지 파트너 솔루션에 대한 요금이 청구되지 않습니다.

## 확장 플랜 파트너 구독 취소

확장 플랜 파트너 솔루션을 더 이상 사용하지 않으려면 파트너 목록에서 구독을 취소할 수 있습니다.

파트너 솔루션 구독을 취소하려면 AWS Marketplace 구매자 안내서의 SaaS 구독 취소 지침을 따르세요.

> **Important**
>
> 구독을 취소하는 것 외에도 회사를 위해 솔루션을 구성한 방법에 따라 파트너 솔루션에 필요한 추가 오프보딩 단계를 따릅니다.

# Security Hub의 교차 리전 집계 이해

Security Hub에서 교차 리전 집계를 활성화하면 홈 리전을 지정합니다. 홈 리전은 하나 이상의 연결된 리전에서 조사 결과, 리소스 및 추세를 수집합니다. 그런 다음 단일 리전에서 모든 보안 데이터를 관리할 수 있습니다.

미국 동부(버지니아 북부)를 홈 리전으로 설정하고 미국 서부(오리건) 및 미국 서부(캘리포니아 북부)를 연결 리전으로 설정한다고 가정해 보겠습니다. 미국 동부(버지니아 북부)의 조사 결과 페이지를 보면 세 리전 모두의 조사 결과를 볼 수 있습니다. 이러한 조사 결과에 대한 업데이트도 세 리전 모두에 반영됩니다.

## 집계되는 데이터 유형

교차 리전 집계가 하나 이상의 연결된 리전으로 활성화되면 Security Hub는 연결된 리전에서 홈 리전으로 다음 데이터를 복제합니다. 이는 교차 리전 집계가 활성화된 모든 계정에서 발생합니다.

- 조사 결과
- 리소스
- Trends

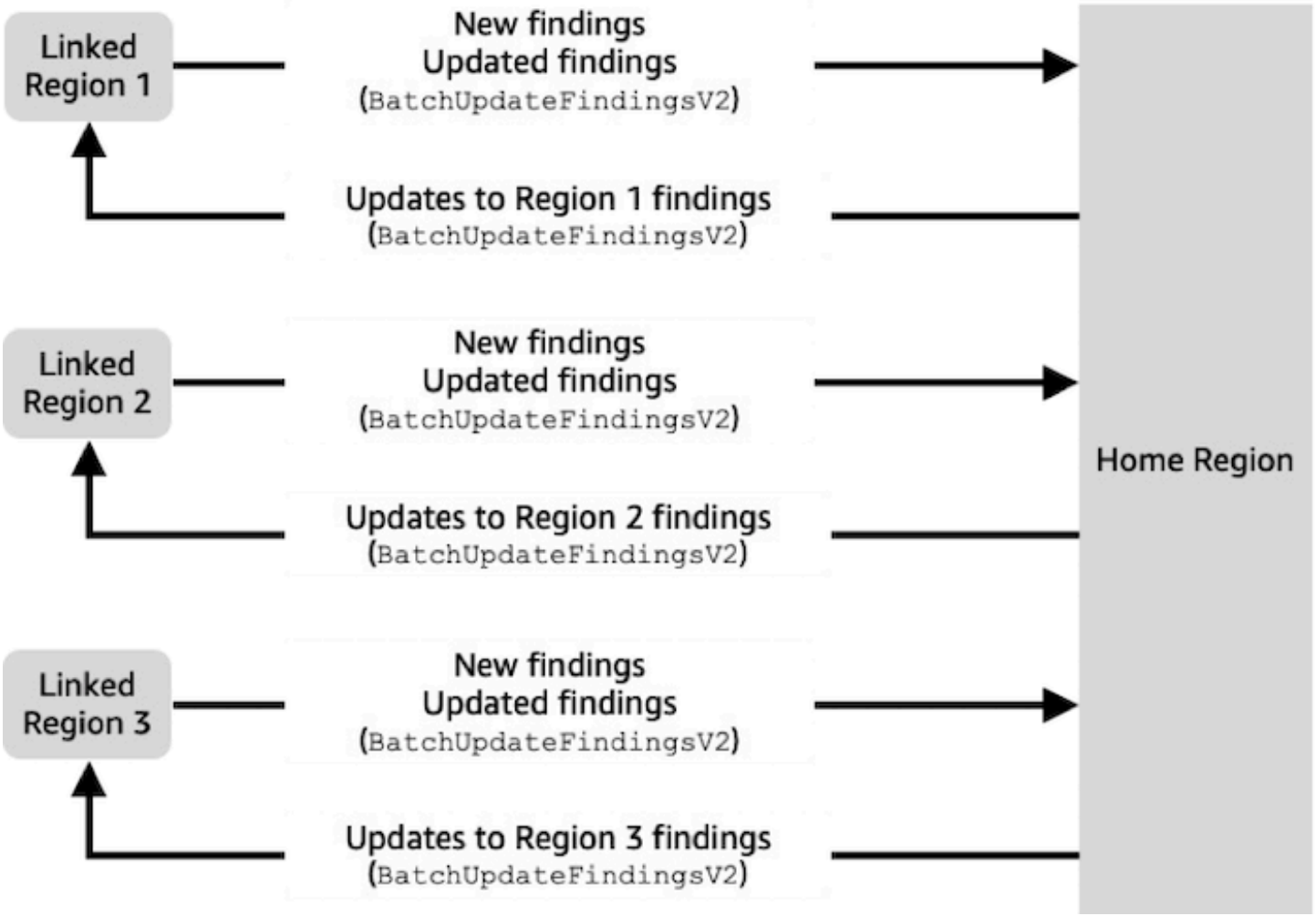
이전 목록의 새로운 데이터 외에 Security Hub는 연결된 리전과 홈 리전 간에 이 데이터에 대한 업데이트를 복제합니다. 연결된 리전에서 발생한 업데이트는 홈 리전에 복제됩니다. 홈 리전에서 발생한 업데이트는 연결된 리전으로 다시 복제됩니다. 집계 영역과 연결 리전의 업데이트가 충돌하는 경우, 가장 최근 업데이트가 사용됩니다.

연결된 리전이 될 때 리전에 있던 모든 결과는 결과에 대한 업데이트가 없는 한 홈 리전에 복제되지 않습니다. 리전이 홈 리전에 연결되면 연결된 리전의 결과가 업데이트되거나 만료될 때까지 홈 리전과 연결된 리전 간에 결과에 차이가 있습니다.

리전이 연결된 리전이 될 때 리전에 있던 모든 리소스는 일반적으로 리전이 홈 리전에 연결된 후 24~48시간 이내에 홈 리전에 복제됩니다.

연결된 리전을 제거할 때 해당 리전의 모든 조사 결과 또는 리소스는 조사 결과 또는 리소스가 만료될 때까지 홈 리전에 남아 있습니다.

추세 데이터는 추세가 속한 리전 내에 있는 조사 결과 및 리소스를 기반으로 합니다. 홈 리전의 추세 데이터는 홈 리전에 동기화된 조사 결과 및 리소스의 현재 상태를 반영합니다.




교차 리전 집계 활성화는 Security Hub 비용에 추가되지 않습니다. Security Hub에서 새로운 데이터나 업데이트를 복제할 때는 요금이 부과되지 않습니다.

홈 리전의 요약 페이지에서는 연결된 리전의 활성 조사 결과 및 리소스를 볼 수 있습니다.

Security Hub는 계정에 Security Hub가 활성화된 리전의 데이터만 집계합니다. Security Hub는 교차 리전 집계 활성화 구성을 기반으로 하는 계정에 대해 자동으로 활성화되지 않습니다.

연결된 리전을 선택하지 않고 교차 리전 집계를 활성화할 수 있습니다. 이 경우, 데이터 복제가 발생하지 않습니다.

## 관리자 및 멤버 계정의 집계

독립 실행형 계정과 관리자 계정은 교차 리전 집계를 구성할 수 있습니다. 관리자가 구성한 경우, 관리형 계정에서 교차 리전 집계가 작동하려면 관리자 계정이 꼭 있어야 합니다. 관리자 계정이 멤버 계정에서 제거되거나 연결 해제되면 해당 멤버 계정에 대한 교차 리전 집계가 중지됩니다. 그러나 관리자와 연결되기 전에 멤버 계정에 자체 리전 간 집계 구성이 있는 경우 해당 구성이 다시 적용됩니다.

관리자 계정이 교차 리전 집계를 활성화하면 Security Hub는 관리자 계정이 연결된 모든 리전에서 관리자 계정이 생성하는 데이터를 홈 리전에 복제합니다. 또한 Security Hub는 해당 관리자와 연결된 멤버 계정을 식별하고 각 멤버 계정은 관리자의 교차 리전 집계 설정을 상속합니다. Security Hub는 멤버 계정이 연결된 모든 리전에서 생성하는 데이터를 홈 리전에 복제합니다.

관리자는 관리되는 리전 내의 모든 멤버 계정에서 보안 조사 결과에 액세스하고 관리할 수 있습니다. 또한 관리자는 관리되는 리전 내의 모든 멤버 계정에서 리소스 인벤토리를 볼 수 있습니다.

Security Hub 멤버 계정으로 홈 리전에 로그인해야 연결된 모든 리전의 계정에서 집계된 데이터를 볼 수 있습니다. 멤버 계정에는 다른 멤버 계정의 데이터를 볼 수 있는 권한이 없으며 `CreateAggregatorV2`, `DeleteAggregatorV2`및 `GetAggregatorV2` APIs를 호출할 수 없습니다.

## 자동화 규칙 및 교차 리전 집계

교차 리전 집계가 활성화된 경우 자동화 규칙은 정의된 홈 리전에서만 생성할 수 있습니다. 규칙 기준이 특정 리전에 적용되지 않는 한 정의한 모든 규칙은 연결된 모든 리전에 적용됩니다. 연결된 리전이 아닌 모든 리전에 대해 별도의 자동화 규칙을 생성해야 합니다.

교차 리전 집계를 활성화하기 전에 홈 리전에서 생성된 모든 규칙은 연결된 리전에서 자동으로 적용됩니다. 연결 리전에서 이전에 생성된 규칙은 애그리게이터가 생성된 후에는 더 이상 적용되지 않습니다. 연결된 리전에 정의된 규칙은 애그리게이터가 삭제되거나 리전이 더 이상 연결되지 않으면 적용이 재개됩니다.

## 교차 리전 집계 활성화 활성화하기

홈 리전으로 지정하려는 AWS 리전에서 교차 리전 집계를 활성화해야 합니다.

교차 리전 집계를 활성화하려면 Security Hub에서 조사 결과 집계자라는 리소스를 생성합니다. 조사 결과 집계자 리소스는 홈 리전 및 연결된 리전(있는 경우)을 지정합니다.

기본적으로 비활성화된 AWS 리전은 홈 리전으로 사용할 수 없습니다. 기본적으로 비활성화된 리전 목록은 AWS 일반 참조의 리전 활성화를 참조하세요.

교차 리전 집계를 활성화할 때 원하는 경우, 하나 이상의 연결된 리전을 지정하도록 선택할 수 있습니다. 교차 리전 집계를 활성화해도 해당 리전에서 Security Hub는 활성화되지 않습니다. 리전에서 Security Hub를 활성화하려면 Security Hub 사용 설명서의 멤버 계정을 관리하기 위한 위임된 관리자로 정책 생성을 참조하세요.

교차 리전 집계를 활성화하려면(콘솔)

1. 관리자 계정 또는 독립 실행형 계정에서 https://console.aws.amazon.com/securityhub/v2/home AWS Security Hub 콘솔을 엽니다.
2. AWS 리전 선택기를 사용하여 집계 리전으로 사용할 리전에 로그인합니다.
3. Security Hub 탐색 메뉴에서 설정을 선택한 다음 일반을 선택합니다.
4. 교차 리전 집계 섹션에서 구성을 선택합니다.
5. 기본적으로, 홈 리전은 집계 리전 없음으로 설정됩니다.
6. 홈 리전에서 현재 리전을 홈 리전으로 지정하는 옵션을 선택합니다.
7. 필요에 따라 연결된 리전에서 데이터를 집계할 리전을 선택합니다.
8. 저장을 선택합니다.

## 교차 리전 집계 설정 검토

관리자 계정 또는 독립 실행형 계정의 모든 AWS 리전에서 AWS Security Hub의 현재 리전 간 집계 구성을 볼 수 있습니다. 멤버 계정은 교차 리전 집계 구성을 볼 수 없습니다. 구성에는 홈 리전과 연결된 리전(있는 경우)이 포함됩니다.

단계에 따라 현재 리전 간 집계 설정을 봅니다.

교차 리전 집계 설정을 보려면(콘솔)

1. https://console.aws.amazon.com/securityhub/v2/home AWS Security Hub 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 일반을 선택합니다.
3. 교차 리전 집계가 활성화되지 않은 경우 일반 페이지에 교차 리전 집계를 활성화하는 옵션이 표시됩니다. 관리자 계정 및 독립 실행형 계정만 교차 리전 집계 활성화를 활성화할 수 있습니다.
4. 교차 리전 집계 활성화가 활성화된 경우, 리전 탭에 다음 정보가 표시됩니다.

- 홈 리전
- Security Hub가 지원하고 사용자가 옵트인한 새 리전의 조사 결과, 리소스 및 추세를 자동으로 집계할지 여부
- 연결된 리전 목록(선택한 경우)

## 교차 리전 집계 설정 업데이트

연결된 리전 또는 현재 홈 리전을 변경하여 AWS Security Hub에서 현재 리전 간 집계 설정을 업데이트할 수 있습니다.

교차 리전 집계에 대한 변경 사항은 AWS 계정에서 리전을 활성화할 때까지 옵트인 리전에 대해 구현되지 않습니다. 2019년 3월 20일 이후에 AWS 도입된 리전은 옵트인 리전입니다.

연결된 리전에서 데이터 집계를 중지하면 AWS Security Hub는 홈 리전에서 액세스할 수 있는 해당 리전에서 기존 집계된 데이터를 제거하지 않습니다.

이 섹션의 업데이트 절차를 사용하여 홈 리전을 변경할 수 없습니다. 홈 리전을 변경하려면 다음을 수행해야 합니다.

1. 현재 교차 리전 집계 구성을 삭제합니다. 지침은 the section called “집계 삭제” 섹션을 참조하세요.
2. 새로운 홈 리전으로 설정하려는 리전으로 변경합니다.
3. 교차 리전 집계 활성화를 활성화 지침은 the section called “집계 활성화” 섹션을 참조하세요.

현재 홈 리전에서 교차 리전 집계 구성을 업데이트해야 합니다.

연결된 리전을 변경하려면(콘솔)

1. 관리자 계정 또는 독립 실행형 계정에서 https://console.aws.amazon.com/securityhub/v2/home AWS Security Hub 콘솔을 엽니다.
2. 현재 집계 전으로 로그인합니다.
3. Security Hub 탐색 메뉴에서 설정을 선택한 다음 일반을 선택합니다.
4. 교차 리전 집계에서 편집을 선택합니다.
5. 연결된 리전의 경우, 선택한 연결된 리전을 업데이트합니다.
6. 저장을 선택합니다.

## 교차 리전 집계 삭제

AWS Security Hub가 데이터를 집계하지 않도록 하려면 결과 집계자를 삭제할 수 있습니다. 또는 연결된 AWS 리전을 선택하지 않도록 기존 애그리게이터를 업데이트하여 조사 결과 애그리게이터를 유지하되 어떤 리전도 홈 리전에 연결하지 않을 수 있습니다.

홈 리전을 변경하려면 현재 조사 결과 집계자를 삭제하고 새로운 집계자를 생성해야 합니다.

조사 결과 집계자를 삭제하면 Security Hub가 데이터 집계를 중지합니다. 홈 리전에서 기존 집계 데이터를 제거하지 않습니다.

조사 결과 집계자 삭제(콘솔)

현재 홈 리전에서만 조사 결과 집계자를 삭제할 수 있습니다.

홈 리전이 아닌 리전의 경우, Security Hub 콘솔의 조사 결과 집계 패널에는 홈 리전의 구성을 편집해야 한다는 메시지가 표시됩니다. 이 메시지를 선택하면 홈 리전으로 전환할 수 있는 링크가 표시됩니다.

교차 리전 집계를 중지하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/v2/home AWS Security Hub 콘솔을 엽니다.
2. 현재 홈 리전에 로그인했는지 확인합니다.
3. Security Hub 탐색 메뉴에서 설정을 선택한 다음 일반을 선택합니다.
4. 교차 리전 집계에서 편집을 선택합니다.
5. 집계 영역에서 집계 영역 없음을 선택합니다.
6. 저장을 선택합니다.
7. 확인 필드의 확인 대화 상자에 **`Confirm`**을 입력합니다.
8. 확인(Confirm)을 선택합니다.

# Security Hub와 Microsoft Azure 통합

Microsoft Azure 리소스를 모니터링하기 위해 Microsoft Azure를 AWS Security Hub와 통합할 수 있습니다. 그런 다음 Security Hub는 Azure 환경에 대한 태세 관리 및 취약성 관리를 자동으로 활성화하고 환경에 대한 조사 결과 및 기타 데이터를 생성합니다. Azure 보안 서비스를 켤 필요는 없습니다. 모든 기능은에서 수행합니다 AWS. 보다 구체적으로, 서비스는 다음을 제공합니다.

CIS Microsoft Azure Foundations Benchmark v4.0 및 Azure 기본 모범 사례

CIS Azure v4.0 표준 및 Azure 기본 모범 사례 표준에 대한 자동화된 규정 준수 검사. 이러한 표준은 자격 증명, 네트워킹, 스토리지, 로깅 및 데이터베이스 제어를 다룹니다.

취약성 관리

Amazon Inspector는 서비스 연결 커넥터를 통해 Azure VMs, 함수 앱 및 Azure 컨테이너 레지스트리(ACR) 컨테이너 이미지에서 소프트웨어 취약성을 자동으로 스캔합니다.

> **Note**
>
> VM 스캔을 사용하려면 Amazon EC2 Systems Manager를 동일한 리전에 구성해야 합니다. 설정 세부 정보는 Azure 통합에 대한 Amazon Inspector 설명서를 참조하세요.

노출 상관 관계

네트워크 연결성, 퍼블릭 액세스 및 잘못된 구성 조합을 기반으로 노출된 Azure 리소스를 자동으로 감지합니다.

Microsoft Defender for Cloud 위협 탐지 알림

Azure Defender를 Event Hub로 지속적으로 내보내도록 구성하면 Security Hub는 클라우드 위협 탐지 알림을 위해 Defender를 수집하고 이를 OCSF(Open Cybersecurity Schema Framework) 형식으로 매핑합니다. 이는 Security Hub 콘솔에서 태세 관리 및 취약성 조사 결과와 함께 표시됩니다.

자산 인벤토리

통합을 통해 검색된 Azure 리소스의 전체 인벤토리로, AWS 리소스와 함께 Security Hub 콘솔에 표시됩니다.

OCSF 형식

Security Hub는 Open Cybersecurity Schema Framework(OCSF) 형식으로 모든 조사 결과를 생성하여 AWS 및 Azure 조사 결과 전반에서 일관된 스키마를 제공합니다.

통합을 생성하려면 다음 프로세스를 통해 Azure 환경을 Security Hub에 연결합니다.

1. 애플리케이션 등록, 페더레이션 자격 증명, Azure 역할 할당 및 Event Hub 인프라를 사용하여 Azure 환경을 구성합니다.

2. Security Hub 콘솔을 사용하여 통합을 위한 커넥터를 생성합니다. Azure 테넌트 ID, 애플리케이션 클라이언트 ID, 모니터링 범위 및 Event Hub 리전을 지정합니다.
3. Security Hub는에 필요한 서비스 연결 역할 및 리소스를 생성합니다 AWS 계정.
4. AWS Config 는 Azure 환경에서 리소스 구성 데이터를 수집합니다.

   AWS Config 는 내부적으로 리소스 구성 데이터를 수집하는 데 사용됩니다. 기록을 명시적으로 활성화하고 비용을 지불해야 하는 태세 관리 AWS Config 와 달리 AWS Azure 태세 관리는 AWS Config 자동으로 처리합니다. 별도로 활성화 AWS Config 하거나, 레코더를 구성하거나, AWS Config 사용량에 대해 별도로 지불할 필요가 없습니다. 이러한 비용은 Security Hub 요금에 포함됩니다.
5. Security Hub는 Azure 환경에서 리소스 구성 데이터 및 활동 로그 이벤트를 수신하기 시작합니다.
6. Security Hub는 Azure 환경에 대한 태세 관리 및 취약성 조사 결과를 생성합니다.

## AWS Config 를 사용하는 방법

AWS Config 는 내부적으로 리소스 구성 데이터를 수집하고 Azure 환경의 변경 사항을 감지하는 데 사용됩니다. 커넥터는 이를 자동으로 처리합니다. AWS Config 별도로를 활성화하거나, 레코더를 구성하거나, AWS Config 사용량을 지불할 필요가 없습니다. 이러한 비용은 Azure 리소스에 대한 Security Hub 요금에 포함됩니다.

## 추가 정보

통합을 생성하면 Security Hub는 Security Hub CSPM 및 Amazon Inspector에서 해당 서비스 연결 통합도 자동으로 생성합니다. 이러한 서비스 연결 통합은 CSPM 검사 및 Inspector 취약성 스캔의 범위가 Security Hub에서 정의한 범위와 일치하는지 확인합니다. 범위를 변경하려면 Security Hub에서 변경해야 합니다. Security Hub CSPM 또는 Inspector에서 직접 서비스 연결 통합을 수정할 수 없습니다.

Security Hub CSPM에서 직접 Azure 통합을 생성하고 독립적인 범위 설정을 지정할 수도 있습니다. 그런 다음 CSPM 통합은 Security Hub 통합과 독립적으로 작동하며 Azure 구독 및 Azure 리전 범위가 다를 수 있습니다.

Security Hub를 Azure와 통합하기 위한 비용 예측 및 계산에 대한 자세한 내용은 AWS Security Hub 요금을 참조하세요.

주제

- Security Hub를 Microsoft Azure와 통합하기 위한 사전 조건
- Security Hub와 통합되도록 Microsoft Azure 구성

- Security Hub를 Microsoft Azure와 통합하도록 구성
- Security Hub에서 Microsoft Azure 커넥터 삭제

# Security Hub를 Microsoft Azure와 통합하기 위한 사전 조건

Microsoft Azure를 AWS Security Hub와 통합하기 전에 및 Azure 환경에서 다음 작업을 AWS 완료합니다. 이렇게 하면 사용자와 Security Hub가 Azure 리소스를 모니터링하는 데 필요한 리소스와 권한을 갖도록 할 수 있습니다.

주제

- 에 대한 사전 조건 AWS
- Microsoft Azure의 사전 조건

## 에 대한 사전 조건 AWS

에 AWS 계정다음이 있는지 확인합니다.

AWS Security Hub 활성화됨

Security Hub는 커넥터를 생성할 AWS 계정 및 AWS 리전 에서 활성화해야 합니다. Azure 커넥터를 생성하기 전에 Security Hub를 활성화해야 합니다.

AWS Security Hub CSPM 활성화

Security Hub CSPM은 동일한 AWS 계정 및에서 활성화되어야 합니다 AWS 리전. Azure 통합은 리소스 구성 평가를 위해 Security Hub CSPM을 사용합니다.

콘솔 IAM 권한

커넥터를 생성하는 IAM 보안 주체에는 다음 권한이 있어야 합니다.

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

IAM 아웃바운드 자격 증명 연동 활성화됨

에서 IAM 아웃바운드 자격 증명 연동을 활성화해야 합니다 AWS 계정. 이 기능을 사용하면 AWS 서비스가 수명이 긴 보안 암호가 아닌 페더레이션 자격 증명을 사용하여 외부 자격 증명 공급자(예: Microsoft Entra ID)에 인증할 수 있습니다.

아웃바운드 자격 증명 연동을 활성화한 후 토큰 발급자 URL을 기록해 둡니다. 이 URL은 형식을 따릅니다.

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

Azure에서 페더레이션 ID 자격 증명을 구성할 때이 URL이 필요합니다.

## Microsoft Azure의 사전 조건

Azure 환경에 다음이 있는지 확인합니다.

Azure 테넌트

Azure 상용 클라우드에 Azure 테넌트가 있어야 합니다. Azure Government 및 Azure China는 지원되지 않습니다.

Microsoft Entra ID 로그 가용성

리소스 기록에는 Microsoft Entra ID 테넌트의 Microsoft Graph 감사 로그 및 로그인 로그가 필요합니다. 일부 Microsoft Entra ID 로그에는 Microsoft Entra ID P1 또는 P2 라이선스가 필요합니다.

테넌트에 필수 로그가 없는 경우 리소스 기록에서 부분 실패를 보고할 수 있습니다. 앱 등록 및 Azure 역할 할당은 누락된 로그 데이터를 제공하지 않습니다.

글로벌 관리자 역할

Azure 환경을 구성하려면 Microsoft Entra ID에 글로벌 관리자 역할이 있어야 합니다. 이 역할은 애플리케이션을 등록하고, Microsoft Graph API 권한에 대한 관리자 동의를 부여하고, 테넌트 루트 관리 그룹 범위에서 RBAC 역할을 할당하고, Entra ID 감사 로그에 대한 진단 설정을 구성하는 데 필요합니다.

통합에 필요한 리소스를 생성하려면 글로벌 관리자 외에도 다음과 같은 Azure RBAC 역할이 필요합니다.

- 루트 범위의 사용자 액세스 관리자(또는 소유자)(/) - 테넌트 루트 관리 그룹 범위에서 RBAC 역할을 할당합니다.
- 테넌트 루트 관리 그룹 범위의 리소스 정책 기여자(또는 소유자) - 진단 설정 및 수정을 자동화하는 Azure 정책 정의 및 할당을 생성합니다.
- Event Hub를 호스팅하는 구독 범위의 기고자(또는 소유자) - Event Hub 네임스페이스 및 관련 리소스를 생성합니다.

> **Note**
>
> 많은 조직에서 Azure 글로벌 관리자와 AWS 보안 관리자는 서로 다른 사람입니다. Azure 설정은 생성된 설정 스크립트를 사용하여 독립적으로 완료할 수 있습니다.

이러한 작업을 완료하면 Azure 환경을 구성할 준비가 된 것입니다.

## Security Hub와 통합되도록 Microsoft Azure 구성

사전 필수 작업을 완료한 후 AWS Security Hub와의 통합을 지원하도록 Microsoft Azure 환경을 구성할 수 있습니다. 이를 위해 Security Hub 콘솔은 구성에 맞게 사용자 지정된 설정 스크립트를 생성합니다.

설정 스크립트를 생성하려면

1. AWS Security Hub 콘솔을 여시겠습니까? https://console.aws.amazon.com/securityhub/advanced/homeregion=us-east-1.
2. 탐색 창에서 통합을 선택합니다.
3. Azure 커넥터 생성을 선택합니다.
4. 커넥터 구성(테넌트 ID, 범위 및 이름)을 완료한 다음 생성된 설정 스크립트를 복사합니다.

스크립트를 실행하려면 Azure CLI를 사용하고 글로벌 관리자 계정()으로 인증합니다`az login`.

스크립트를 실행하면 일련의 작업이 수행됩니다. 다음 섹션에서는 스크립트가 수행하는 각 작업에 대해 설명합니다. 조직에서 스크립트 실행을 제한하는 경우이 주제를 지침으로 사용하여 이러한 작업을 수동으로 수행할 수 있습니다. Azure 환경을 구성한 후 Azure와 통합하도록 Security Hub를 구성할 수 있습니다.

1~7단계는 애플리케이션 등록, 페더레이션 자격 증명, Azure 역할 할당, Microsoft Graph 권한, Event Hub 및 로그 내보내기 등 모든 Security Hub 기능이 사용하는 공유 기반을 구성합니다. 8~10단계는 특정 기능에 대한 추가 Azure 리소스를 구성합니다.

- 취약성 관리(Amazon Inspector) - Azure VMs에서 Azure 컨테이너 레지스트리(ACR) 리포지토리 이벤트 내보내기 및 시스템 할당 관리형 ID를 구성합니다.
- 위협 탐지(클라우드용 Microsoft Defender) - 보안 알림을 Event Hub로 지속적으로 내보내도록 클라우드용 Microsoft Defender를 구성합니다.

> **Note**
>
> 단일 Azure 앱 등록은 AWS 보안 서비스 간에 공유됩니다. 또한 Security Hub CSPM 또는 Azure용 Amazon Inspector를 사용하는 경우 동일한 앱 등록을 사용합니다. 각 AWS 서비스에 대해 별도의 등록을 생성할 필요는 없습니다.

작업

- 1단계: Azure 애플리케이션 등록
- 2단계: 서비스 보안 주체 생성
- 3단계: 페더레이션 자격 증명 구성
- 4단계: RBAC 역할 할당
- 5단계: Microsoft Graph API 권한 구성
- 6단계: Azure Event Hub 설정
- 7단계: 활동 로그 및 Entra ID 감사 로그 내보내기 구성
- 8단계: Azure 컨테이너 레지스트리 내보내기 구성
- 9단계: Azure VMs에서 관리형 자격 증명 활성화
- 10단계: 클라우드 알림을 위해 Microsoft Defender 내보내기

## 1단계: Azure 애플리케이션 등록

Microsoft Entra ID에 새 애플리케이션을 등록합니다. 이 애플리케이션은가 연합 자격 증명을 사용하여 Azure 환경에 인증하는 데 AWS 사용하는 자격 증명 역할을 합니다. 클라이언트 보안 암호는 필요하지 않습니다.

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

출력의 애플리케이션(클라이언트) ID(`appId`속성)를 기록해 둡니다. Security Hub 콘솔에서 커넥터를 생성할 때이 값을 제공합니다.

## 2단계: 서비스 보안 주체 생성

등록된 애플리케이션에 대한 서비스 보안 주체를 생성합니다. Azure 역할 할당을 사용하여 서비스 보안 주체에 권한을 부여합니다. 서비스 보안 주체는 Azure 환경에서 작업을 수행합니다.

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

여기서 *application-client-id*는 이전 단계의 애플리케이션(클라이언트) ID입니다.

등록 시 애플리케이션 ID URI를 로 설정합니다`api://`*application-client-id*.는 페더레이션 토큰을 애플리케이션과 교환하려면이 식별자가 AWS 필요합니다. 이 URI가 없으면가 유효한 페더레이션 토큰 대상을 생성할 AWS 수 없으며 모든 기능이 Azure에 인증하지 못합니다.

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

### 3단계: 페더레이션 자격 증명 구성

가 클라이언트 보안 암호 없이 인증할 AWS 수 있도록 애플리케이션에서 페더레이션 자격 증명을 구성합니다. 이렇게 하면 AWS 와 Azure 간에 OIDC 신뢰가 설정됩니다. 수명이 긴 보안 암호 또는 자격 증명은 저장되지 않습니다.

Security Hub Azure 통합은 리소스 구성 검색, 취약성 관리 및 위협 탐지 기능당 하나의 AWS IAM 역할을 사용하여 인증합니다. 모든 기능이 Azure에 인증할 수 있도록 각 역할에 페더레이션 자격 증명을 추가합니다. AWS 는 커넥터를 생성할 때 서비스 연결 역할을 자동으로 생성합니다. VM 스캔에 `Inspector2SSMFederationRole` 사용되는는 서비스 연결 역할이 아닙니다. 9단계에 설명된 Amazon Inspector VM 스캔 설정의 일부로 생성합니다.

| 기능 | 제목(IAM 역할 ARN) |
| --- | --- |
| 리소스 구성 검색(AWS Config) | `arn:aws:iam::` *account-id* `:role/aws-service-role/thirdparty.config.amazonaws.com/AWSServiceRoleForConfigThirdParty` |
| 취약성 관리(조사자) | `arn:aws:iam::` *account-id* `:role/aws-service-role/thirdparty.inspector2.amazonaws.com/AWSServiceRoleForAmazonInspector2ThirdParty` |
| 취약성 관리 - VM 스캔(Amazon EC2 Systems Manager) | `arn:aws:iam::` *account-id* `:role/Inspector2SSMFederationRole-` *tenant-id* |

| 기능 | 제목(IAM 역할 ARN) |
| --- | --- |
| 위협 탐지(Security Hub) | arn:aws:iam:: *account-id* :role/aws-service-role/securityhubv2.amazonaws.com/AWSServiceRoleForSecurityHubV2 |

위 표의 각 제목에 대해 다음 명령을 한 번 실행하여 매번 name 및 subject 값을 변경합니다. issuer 및 audiences 값은 모든 자격 증명에 대해 동일합니다.

```
$ 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"
  }'
```

키 값:

- 발급자 - IAM 아웃바운드 자격 증명 연동의 토큰 발급자 URL입니다. 형식에 따릅니다https://*uuid*.tokens.sts.global.api.aws.
- 제목 - 이전 테이블의 IAM 역할 ARN입니다. Amazon EC2 Systems Manager 역할의 *### ID*는 Azure 테넌트 ID입니다.
- 대상 - api://AzureADTokenExchange (워크로드 자격 증명 페더레이션의 표준 값).
- 이름 - 애플리케이션 내에서 고유한 모든 이름입니다.

## 4단계: RBAC 역할 할당

서비스 보안 주체에 다음과 같은 기본 제공 역할을 할당합니다.

- 리더 - Security Hub가 리소스 구성을 검색하고 평가할 수 있도록 모든 Azure 리소스에 대한 읽기 전용 액세스 권한을 부여합니다. 루트 범위(/)에서이 역할을 할당합니다.
- 기여자 - Amazon Inspector가 Azure 가상 머신, 함수 앱 및 컨테이너 이미지의 취약성을 스캔하는 데 필요한 쓰기 액세스 권한을 부여합니다. 테넌트의 모든 구독에 전파되는 테넌트 루트 관리 그룹 범위에이 역할을 할당합니다.

- Azure Event Hubs 데이터 수신기 -가 Event Hub에서 이벤트를 읽을 수 있도록 허용합니다 AWS . 테넌트 루트 관리 그룹 범위에서이 역할을 할당합니다.

> ⚠ 루트 범위에서 리더 할당
>
> 테넌트 루트 관리 그룹 범위가 아닌 루트 범위(/)에서 리더 역할을 할당해야 합니다. Security Hub는 테넌트 루트에 범위가 지정된 할당을 포함하여 모든 범위에서 Azure 역할 할당 리소스를 읽습니다. 루트 관리 그룹의 리더 할당은 범위가 인 할당을 다루지 않으므로 /읽기가 실패하고 권한 부여 오류로 인해 커넥터가 성능 저하 상태가 될 수 있습니다.

> ⚠ 기고자를 통해 테넌트 전체의 쓰기 액세스 권한 부여
>
> 테넌트 루트 관리 그룹 범위의 기여자 역할은 Azure 리소스에 대한 권한이 높은 테넌트 전체 쓰기 액세스 권한을 부여합니다. Amazon Inspector가 컴퓨팅 리소스의 취약성을 스캔할 수 있도록 Security Hub에이 액세스 권한이 필요합니다. 예를 들어 Inspector는 Contributor가 제공하는 가상 머신 실행 명령 권한을 사용합니다. Amazon EC2 Systems Manager Automation을 통해 Inspector는 Azure VMs에서 명령을 실행하여 VM 스캐너 에이전트를 설치하고 운영합니다.

```
$ 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 "/"
```

> **루트 범위 할당에는 승격된 액세스가 필요합니다.**
>
> 루트 범위(/)에서 역할을 할당하려면 승격된 액세스 권한이 필요합니다. 역할 할당에 실패하면 Microsoft Entra ID > 속성에서 Azure 리소스에 대한 액세스 관리가 예로 설정되어 있는지 확인합니다. 그런 다음 로그아웃했다가 다시 로그인하여 토큰을 새로 고칩니다.

> **임시 루트 고도 제거**
>
> Azure 리소스에 대한 액세스 관리를 활성화하면 로그인한 관리자에게 루트 범위(/)의 사용자 액세스 관리자 역할이 부여되며,이 역할은 테넌트의 모든 구독 및 관리 그룹에서 액세스를 관리할 수 있습니다. 온보딩이 완료되면 Azure 리소스에 대한 액세스 관리를 Microsoft Entra ID > 속성에서 아니요로 다시 설정하여이 고도가 활성 상태로 유지되지 않도록 합니다.

### 5단계: Microsoft Graph API 권한 구성

애플리케이션에 다음 Microsoft Graph API 권한(애플리케이션 유형)을 부여한 다음 관리자 동의를 부여합니다.

- `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
```

## 6단계: Azure Event Hub 설정

AWS Config 는 Azure Event Hub를 사용하여 Azure 환경의 리소스 구성 변경 사항에 대한 알림을 거의 실시간으로 수신합니다. 설정 스크립트는 Event Hub 인프라를 생성하고 검색을 위해 태그를 지정합니다. Event Hub 검색은 태그 기반 확인을 사용합니다. Security Hub는 형식의 Event Hub 네임스페이스에서 태그를 찾아 통합`AWSConfig-`*`account-id`*`-`*`region`*에 적합한 Event Hub 인스턴스를 식별합니다.

```
$ 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"
```

Event Hub를 생성한 후 검색할 네임스페이스에 태그를 지정하고 데이터 수신자 역할을 할당합니다. 네임스페이스에 다른 태그(예: 10단계의 위협 탐지 검색 태그)를 보존`--operation merge`하려면 `az tag update`와 함께를 사용합니다.

```
$ 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**
>
> 태그 형식에서 AWSConfig-*account-id*-*region* *account-id*는 12자리 AWS 계정 ID이고 *region*은 커넥터를 생성하는 AWS 리전 입니다(예: us-east-1). 이러한 값은이 Event Hub 통합을 소유한 AWS 계정 및 리전을 식별합니다.

주요 구성:

- 네임스페이스 SKU - 표준(소비자 그룹에 필요).
- Event Hub 이름 - activitylog.
- 소비자 그룹 - AWSConfig.
- 태그 - AWSConfig-*account-id*-*region* 값이 있는 입니다activitylog. 이 태그를 사용하면 AWS Config 가 Event Hub를 자동으로 검색할 수 있습니다.
- 역할 할당 - 네임스페이스의 Azure Event Hubs 데이터 수신기입니다.

위협 탐지를 위해 설정은 AWSSecurityHub 소비자 그룹과 함께 별도의 defender-alerts Event Hub를 생성하고 Security Hub가 직접 읽AWSSecurityHub-*account-id*-*region*는 허브를 식별하는 형식으로 두 번째 검색 태그를 추가합니다. 자세한 내용은 10단계를 참조하세요.

## 7단계: 활동 로그 및 Entra ID 감사 로그 내보내기 구성

활동 로그와 Microsoft Entra ID 로그를 Event Hub로 내보내도록 Azure를 구성합니다.

활동 로그 내보내기:

각 구독에 대한 진단 설정을 구성하여 활동 로그를 Event Hub로 내보냅니다. 설정 스크립트는 모니터링되는 모든 구독에 대해 이를 자동으로 구성합니다. 활동 로그는 역할 할당 및 리소스 변경을 포함한 구독 수준 활동을 캡처합니다.

Microsoft Entra ID 로그 내보내기:

Microsoft Entra ID에서 진단 설정을 구성하여 로그를 동일한 Event Hub로 내보냅니다. Microsoft Entra ID > 모니터링 > 진단 설정 > 진단 설정 추가로 이동합니다. AuditLogs, SignInLogs 및 NonInteractiveUserSignInLogs를 활성화하고 Event Hub로 라우팅합니다.

### 8단계: Azure 컨테이너 레지스트리 내보내기 구성

Security Hub는 Amazon Inspector를 통해 Azure 컨테이너 레지스트리(ACR) 컨테이너 이미지의 취약성을 스캔합니다. 이를 위해 Inspector는 레지스트리와 동일한 Azure 리전의 Event Hub로 내보낸 ACR 리포지토리 이벤트가 필요합니다. ACR 내보내기 설정은 Amazon Inspector 사용 설명서의 Microsoft Azure와 통합하도록 Amazon Inspector 구성을 참조하세요.

### 9단계: Azure VMs에서 관리형 자격 증명 활성화

Security Hub는 Inspector를 통해 Azure 가상 머신을 스캔합니다. 각 대상 Azure VM에는 시스템에서 할당한 관리형 ID가 활성화되어 있어야 합니다. VMs 자동으로 추가하려면 테넌트 루트 관리 그룹 범위에서 `modify` 효과를 사용하는 두 개의 Azure 정책을 할당합니다.

- 자격 증명이 없는 VM의 경우 정책은 시스템에서 할당한 관리형 자격 증명을 추가합니다.
- 사용자 할당 자격 증명만 있는 VM의 경우 정책은 기존 사용자 할당 자격 증명을 유지하면서 시스템 할당 관리형 자격 증명을 추가합니다.

이미 시스템에 할당된 관리형 ID가 있는 VM은 변경되지 않습니다. 정책은 `modify` 효과를 사용하므로 VM을 재배포하지 않고 자격 증명을 제자리에 조정합니다.

Inspector는 Amazon EC2 Systems Manager Automation을 사용하여 Azure VM에서 Inspector VM 스캐너 에이전트를 배포하고 관리합니다 VMs. 이를 위해서는 Microsoft Entra ID용 IAM OIDC 자격 증명 공급자와 여러 IAM 역할을 포함한 추가 AWS측 설정이 필요합니다. 전체 VM 스캔 설정은 Amazon Inspector 사용 설명서의 Microsoft Azure와 통합하도록 Amazon Inspector 구성을 참조하세요.

### 10단계: 클라우드 알림을 위해 Microsoft Defender 내보내기

Security Hub는 Microsoft Defender for Cloud 위협 탐지 알림을 수집하여 OCSF(Open Cybersecurity Schema Framework) 형식으로 매핑합니다. 이러한 알림을 전달하려면 전용 `defender-alerts` Event Hub를 생성하고 클라우드용 Microsoft Defender를 구성하여 보안 알림을 클라우드로 지속적으로 내보냅니다.

6단계의 Event Hub 네임스페이스에서 Event Hub, Security Hub가 읽을 `AWSSecurityHub` 소비자 그룹, Microsoft Defender for Cloud가 알림을 보내는 데 사용하는 전송 권한이 있는 허브 범위의 공유 액세스 서명(SAS) 권한 부여 규칙을 생성합니다. `defender-alerts`

```
$ 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
```

그런 다음 Security Hub가 `defender-alerts` 허브를 검색하도록 두 번째 검색 태그를 네임스페이스에 병합합니다. 6단계의 `AWSConfig` 검색 태그를 보존`--operation merge`하려면 `az tag update`와 함께를 사용합니다. ???

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

마지막으로 보안 알림 데이터 유형을 `defender-alerts` Event Hub로 클라우드로 지속적으로 내보내도록 Microsoft Defender를 구성합니다. Azure 포털에서 Microsoft Defender for Cloud > 환경 설정으로 이동하여 구독을 선택하고 연속 내보내기 > Event Hub를 선택한 다음 보안 알림을 선택하고 `defender-alerts` Event Hub 및 `DefenderExportSend` SAS 규칙을 선택합니다.

> **Note**
>
> 포털이 아닌 프로그래밍 방식으로(Azure Resource Manager API, ARM 템플릿 또는 Azure 정책을 통해) 연속 내보내기를 구성하는 경우 `DefenderExportSend` SAS 연결 문자열을 사용하여 Event Hub로 내보내기를 인증합니다. `DefenderExportSend` 규칙에 `az eventhubs eventhub authorization-rule keys list` 대해를 사용하여 검색하고 내보내기 작업의 연결 문자열로 설정합니다. 자세한 내용은 Microsoft Azure 설명서의 지속적 내보내기 설정을 참조하세요.

> **Note**
>
> 이러한 작업을 완료한 후 구성이 적용될 때까지 약 15~30분 정도 기다립니다. 그런 다음 Security Hub에서 커넥터를 생성하기 전에 Event Hub가 메시지(IncomingMessages 지표)를 수신하고 있는지 확인합니다.

## Security Hub를 Microsoft Azure와 통합하도록 구성

사전 필수 작업을 완료하고 Microsoft Azure 환경을 구성한 후 Azure와 통합하도록 AWS Security Hub를 구성할 수 있습니다. Azure와 통합되도록 Security Hub를 구성하려면 커넥터를 생성합니다. 위임된 관리자 계정 또는 관리 계정에서 커넥터를 생성할 수 있습니다. 커넥터를 생성한 후 다음 이벤트가 발생합니다.

1. Security Hub는 Azure 자격 증명과 Azure 환경에 대한 연결을 검증합니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다.
2. Security Hub는 Security Hub CSPM 및 Amazon Inspector에서 서비스 연결 커넥터를 생성합니다. 이러한 커넥터는 태세 관리 검사 및 취약성 스캔이 Security Hub에서 정의한 범위와 일치하는지 확인합니다.
3. AWS Config 는 페더레이션 자격 증명을 사용하여 Azure 리소스 검색을 시작합니다.
4. Security Hub는 Azure 리소스에 대해 CSPM에서 CIS Microsoft Azure Foundations Benchmark v4.0 표준 및 Azure Foundational Best Practices 표준을 자동으로 활성화합니다.
5. 초기 결과는 활동 로그 이벤트가 있는 리소스에 대해 15~30분 이내에 나타나기 시작합니다. 모든 기존 리소스에 대한 전체 평가는 최대 24시간이 걸릴 수 있습니다.

주제

- Azure 커넥터 생성
- Azure 커넥터의 범위 조정
- Azure 커넥터의 상태 확인
- Azure 커넥터 문제 해결
- Security Hub가 리소스 및 조사 결과 식별자를 처리하는 방법

## Azure 커넥터 생성

환경에 맞는 Microsoft Azure 커넥터를 생성하려면 AWS Security Hub 콘솔 또는 API를 사용하여 다음 단계를 완료합니다.

1. AWS Security Hub 콘솔을 여시겠습니까? https://console.aws.amazon.com/securityhub/advanced/homeregion=us-east-1.
2. 탐색 창에서 통합을 선택합니다.
3. Azure 커넥터 생성을 선택합니다.
4. 보안 기능 섹션에서 네트워크 스캔 기능을 활성화할지 여부를 선택합니다. 이 기능은 Azure 통합을 활성화하는 계정에 대해 기본적으로 활성화되며 커넥터 설정을 완료하기 전에 선택을 취소할 수 있습니다. 조직 정책이 계정에 대해이 기능을 차단하는 경우 옵션으로 표시되지 않습니다. 자세한 내용은 Security Hub의 네트워크 스캔을 참조하세요.
5. Azure 테넌트 ID에 Microsoft Entra ID 테넌트 식별자를 입력합니다. Azure 포털의 Microsoft Entra ID > 속성 > 테넌트 ID에서 찾을 수 있습니다.
6. 애플리케이션(클라이언트) ID에 Azure 환경 설정 중에 등록한 Azure 애플리케이션의 애플리케이션 ID를 입력합니다.
7. 다음을 수행하여 추가 설정과 커넥터 범위를 구성합니다.

   - 이름에 커넥터의 고유한 이름을 입력합니다. 이름은 최대 50자의 영숫자를 포함할 수 있으며 하이픈을 포함할 수 있습니다.

     > **Note**
     >
     > 커넥터 이름은 생성 후 변경할 수 없습니다.

   - 설명에 필요에 따라 커넥터에 대한 간략한 설명을 입력합니다. 설명은 최대 200자를 포함할 수 있습니다.

     > **Important**
     >
     > 이름과 설명은 콘텐츠를 식별하는 데 사용됩니다. 민감한 정보, 기밀 정보 또는 개인 식별 정보(PII)를 포함하지 마십시오.

- 구독에서 모든 구독을 선택하여 테넌트의 모든 현재 및 미래 구독을 모니터링하거나 특정 구독을 선택하여 지정한 구독만 모니터링합니다. 특정 구독만 모니터링하도록 선택한 경우 각 구독의 ID를 입력합니다.
- 리전에서 모든 Azure 리전의 리소스를 모니터링하려면 모든 리전을 선택하고, 지정한 리전만 모니터링하려면 특정 리전을 선택합니다.

> **Note**
>
> 동일한 Azure 테넌트에 대해 Security Hub CSPM 또는 Amazon Inspector에서 커넥터를 이미 생성한 경우 Security Hub의 커넥터 범위에는 Security Hub CSPM 또는 Amazon Inspector의 커넥터와 동일한 구독 및 리전이 포함되어야 합니다.

> **Note**
>
> Microsoft Entra ID 및 Microsoft Graph 리소스를 평가하는 컨트롤을 사용하려면 통합 구성에 글로벌 리전 범위를 포함해야 합니다. 특정 Azure 리전만 선택하는 경우 이러한 제어는 결과를 생성하지 않습니다.

8. 커넥터 구성을 검토합니다.

> **Note**
>
> Azure VM 스캔에 Amazon Inspector를 사용하려는 경우 필요한 IAM 역할을 생성해야 합니다. 자세한 내용은 the section called “VM 스캔을 위한 IAM 역할”을 참조하세요.

9. 설정 입력 및 검토를 마치면 커넥터 생성을 선택합니다.

Amazon Inspector를 통한 Azure VM 스캔을 위한 IAM 역할

Amazon Inspector를 통해 취약성 스캔을 활성화하려면에서 다음 IAM 리소스를 생성해야 합니다 AWS 계정.

IAM OIDC 자격 증명 공급자

다음 구성으로에 대한 IAM OIDC 자격 증명 공급자를 생성합니다Microsoft Entra ID.

- 발급자 URL: `https://sts.windows.net/tenant-id/`
- 클라이언트 ID 목록: `api://app-id`, `api://AzureADTokenExchange`
- 지문: 0의 40자 문자열입니다(040회 반복). AWS STS 는 지문 값이 아닌 JWKS 엔드포인트를 통해 토큰을 검증합니다.

### Inspector2VmScannerRole-*tenant-id*

Azure VM에서 실행되는 Amazon Inspector VMs 스캐너 에이전트가 스캔 원격 측정을 Amazon Inspector로 전송하는 데 사용됩니다. 이 역할은 자격 증명 공급자를 통해 OIDC 웹 Microsoft Entra ID 자격 증명 페더레이션을 사용합니다.

신뢰 정책:

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

태그:

- `inspector-managed = true`

권한 정책(TelemetryPolicy):

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

```
        }
    ]
}
```

Inspector2SSMFederationRole-*tenant-id*

안전한 클라우드 간 인증을 위해 Azure에 대한 OIDC 페더레이션을 활성화합니다. 이 역할은 Azure 작업에 대한 웹 자격 증명 토큰을 얻기 위해 AssumeRole 및 DispatchRole과 Amazon EC2 Systems Manager에서 수임합니다.

신뢰 정책:

```
{
    "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"
        }
    ]
```

```
}
```

권한 정책(FederationPolicy):

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

태그:

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

### Inspector2SSMAssumeRole-*tenant-id*

Amazon EC2 Systems Manager Automation을 실행하여 Azure VMs 관리형 인스턴스로 온보딩합니다. 이 역할은 하이브리드 활성화를 생성 및 관리하고, Amazon EC2 Systems Manager에 역할을 전달하고, 자동화 문서를 검색합니다.

신뢰 정책:

```
{
    "Version":"2012-10-17",
    "Statement": [
```

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

권한 정책(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": "*"
        }
    ]
}
```

태그:

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

### Inspector2SSMDispatchRole-*tenant-id*

Amazon EC2 Systems Manager Automation을 통해 Azure VM 대상을 해결하고 Amazon Amazon Inspector VM 스캐너 에이전트 설치를 디스패치합니다. 이 역할은 자동화 실행을 시작하고 AssumeRole을 Amazon EC2 Systems Manager에 전달합니다.

신뢰 정책:

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

권한 정책(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": "*"
        }
    ]
}
```

태그:

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

VM 스캔을 위한 사전 조건

Azure 앱 등록에는 애플리케이션 ID URI가 로 설정되어 있어야 합니다`api://app-id`.

스캔하려는 각 Azure VM에는 시스템에서 할당한 관리형 ID가 활성화되어 있어야 합니다. 새 VMs에 관리형 자격 증명을 자동으로 할당하려면 Azure 환경에서 DeployIfNotExists 정책을 사용합니다.

커넥터를 생성한 후 Security Hub는 Azure 환경 모니터링을 시작합니다. 통합 페이지에서 커넥터의 상태를 확인할 수 있습니다.

## Azure 커넥터의 범위 조정

Microsoft Azure 커넥터를 생성한 후 모니터링하는 Azure 구독 또는 Azure 리전을 변경하여 커넥터의 범위를 조정할 수 있습니다. 범위 변경은 일반적으로 활동 로그 이벤트가 있는 리소스에 대해 15~30분 이내에 적용됩니다. 새로 추가된 Azure 구독에 대한 전체 평가는 최대 24시간이 걸릴 수 있습니다.

커넥터의 범위를 조정하기 전에 다음 사항에 유의하세요.

- Security Hub에서 커넥터의 범위를 변경하면 Security Hub CSPM 및 Amazon Inspector의 연결된 서비스 연결 커넥터가 일치하도록 자동으로 업데이트됩니다.
- Security Hub 커넥터의 범위는 동일한 Azure 테넌트에 대한 Security Hub CSPM 또는 Amazon Inspector의 기존 고객 관리형 커넥터보다 작을 수 없습니다.
- 커넥터 범위에 리전을 추가하는 경우 설정 스크립트를 다시 실행하여 새 리전에서 Event Hub 인프라를 프로비저닝해야 합니다. 기존 Event Hub 구성은 영향을 받지 않습니다.

## Azure 커넥터의 상태 확인

언제든지 Microsoft Azure 커넥터의 상태를 확인하여 Security Hub가 Azure 환경에서 데이터를 수신하고 있는지 확인할 수 있습니다.

커넥터의 상태를 확인하려면

1. AWS Security Hub 콘솔을 여시겠습니까? https://console.aws.amazon.com/securityhub/advanced/homeregion=us-east-1.
2. 탐색 창에서 통합을 선택하고 Azure 커넥터를 선택합니다.
3. 커넥터 상태가 활성으로 표시되는지 확인합니다. 커넥터에 활성이 표시되면 확인이 완료된 것입니다. 다른 상태가 표시되면 섹션을 참조하세요the section called “커넥터 문제 해결”.
4. 조사 결과 및 필터링 기준으로 이동하여 Azure 리소스`ResourceCloudProviders = Azure`에 대한 조사 결과가 생성되고 있는지 확인합니다.
5. 보안 표준 페이지를 확인하여 CIS Azure v4.0 표준에 PASSED 또는 FAILED 상태(일부 NO_DATA는 아님)의 제어가 표시되는지 확인합니다.

> **Note**
>
> 커넥터 상태는 최종적으로 일관됩니다. 권한 또는 구성 문제가 발생하면 커넥터 상태가 실행 가능한 메시지와 함께 빠르게 성능 저하로 변경됩니다. 그러나 문제를 해결한 후 상태가 연결됨으로 돌아가는 데 최대 24시간이 걸릴 수 있습니다.

- 최근 수정 후 성능 저하 상태가 반드시 지속적인 문제를 나타내는 것은 아닙니다.
- 레코딩 실패에 대한 실시간 가시성을 얻으려면 네임스페이스에서 CloudWatch 지표를 확인하세요.

## Azure 커넥터 문제 해결

커넥터에 문제가 발생하면 다음과 같은 일반적인 문제와 해결 방법을 검토하세요.

커넥터 상태가 비정상임

이 문제는 일반적으로 Azure에서 페더레이션 자격 증명이 올바르게 구성되지 않은 경우에 발생합니다.

이 문제를 해결하려면 Azure 페더레이션 자격 증명의 토큰 발급자 URL 및 주제 ARN이와 일치하는지 확인합니다 AWS 계정.

30분 후 결과 없음

이 문제는 Event Hub가 활동 로그를 수신하지 않는 경우 발생할 수 있습니다.

이 문제를 해결하려면 Azure 구독에 진단 설정이 구성되어 있고 Event Hub 네임스페이스에 로 태그가 올바르게 지정되어 있는지 확인합니다`AWSConfig-`*`account-id`*`-`*`region`*.

모든 컨트롤에 NO_DATA 표시

이 문제는 커넥터가 비활성화되어 있거나가 Azure 환경에 도달할 수 AWS Config 없는 경우에 발생할 수 있습니다.

이 문제를 해결하려면 커넥터가 활성화되어 있고 서비스 보안 주체가 테넌트 루트 관리 그룹 범위에 리더 역할을 가지고 있는지 확인합니다.

일부 Azure 리소스를 기록할 수 없음

오류는 다음과 같은 이유로 발생할 수 있습니다.

- Azure 환경이 리소스 기록을 위한 사전 조건을 충족하지 않습니다.
- 앱 등록에는 Microsoft Graph API 권한에 대한 관리자 동의가 없습니다.
- 리더 역할 할당에 필요한 모든 범위가 포함되지는 않습니다.
- Microsoft Entra ID 테넌트에 필요한 로그 데이터가 없습니다.

오류를 해결하려면 다음을 수행합니다.

1. 환경이 모든 요구 사항을 충족하는지 확인하려면 Microsoft Azure의 사전 조건을 검토하세요.
2. 앱 등록에 관리자의 동의를 받아 필요한 Microsoft Graph API 권한이 있는지 확인합니다.
3. 서비스 보안 주체가 테넌트 루트 관리 그룹 범위에 리더 역할을 가지고 있는지 확인합니다.

조사 결과는 일부 구독에만 표시됩니다.

이 문제는 활동 로그 내보내기가 모든 대상 구독에 대해 구성되지 않은 경우 발생할 수 있습니다.

이 문제를 해결하려면 진단 설정이 커넥터 범위에 포함된 모든 구독을 포함하는지 확인합니다.

### Security Hub가 리소스 및 조사 결과 식별자를 처리하는 방법

AWS Security Hub용 Azure 통합을 활성화하면 다른 클라우드 공급자의 리소스 및 보안 조사 결과 식별자가 다른 AWS 클라우드 공급자로부터 수집된 해당 리소스 구성 및 보안 조사 결과 데이터의 관리와 관련된 메타데이터로 AWS Config Security Hub 및 기타 서비스(필요한 경우)에 저장됩니다. 이러한 식별자는 사용자의 콘텐츠를 구성하지 않습니다. 민감한 정보, 기밀 정보 또는 개인 식별 정보를 포함하지 마세요.

연결된 클라우드 환경의 다음 식별자는에서 멀티클라우드 보안 기능을 제공하기 AWS 위해 저장 및 사용됩니다.

- 리소스 식별자: Azure 테넌트 ID, 구독 ID, 위치(리전), 리소스 ID(리소IDs 또는 이름, 리소스 공급자, 리소스 유형)
- Security Finding 식별자: 감지 서비스에서 생성된 각 보안 결과에 할당된 고유 식별자입니다.

리소스가 서로 연관되는 방식과 조사 결과가 리소스와 연관되는 방식을 포함하여 이러한 식별자 간의 관계는 서비스 메타데이터로도 저장됩니다.는 조사 결과를 리소스, 서비스 운영 로깅 및 중복 제거에 연결하여 리소스 상관 관계를 위해 이러한 식별자를 AWS 사용합니다.

## Security Hub에서 Microsoft Azure 커넥터 삭제

AWS Security Hub에서 Microsoft Azure 커넥터를 생성한 후 언제든지 삭제할 수 있습니다. 커넥터를 삭제하면 Security Hub는 Azure 환경에 대한 태세 관리 검사 및 취약성 모니터링 수행을 중지합니다. 또한 Security Hub는 환경에 대한 새 조사 결과 및 기타 데이터 생성을 중지합니다. 기존 결과는 90일 동안 보존됩니다. 리소스 인벤토리는 커넥터가 삭제되고 90일 후에 제거될 때와 동일하게 유지됩니다.

커넥터를 삭제하면 Security Hub는 AWS Security Hub CSPM 및 Amazon Inspector에서 연결된 서비스 연결 커넥터를 자동으로 삭제합니다. Security Hub는 Azure 환경에서 Azure 애플리케이션 등록 및

Event Hub 인프라를 삭제하지 않습니다. Microsoft Azure에서 직접 수동으로 삭제해야 합니다. 자세한 내용은 Microsoft Azure 설명서의 애플리케이션 제거를 참조하세요.

Azure 커넥터를 삭제하려면

1. AWS Security Hub 콘솔을 여시겠습니까? https://console.aws.amazon.com/securityhub/advanced/homeregion=us-east-1.
2. 탐색 창에서 통합을 선택합니다.
3. 삭제할 커넥터를 선택합니다.
4. 삭제를 선택합니다.
5. 메시지가 표시되면 커넥터를 삭제할지 확인합니다.

> **Important**
>
> 커넥터를 삭제하고 6시간 이내에 새 커넥터를 생성하는 경우 리소스 감지에 최대 6시간이 걸릴 수 있습니다. 그에 따라 커넥터 삭제 및 재생성을 계획합니다.

# Security Hub의 요약 대시보드에서 작업

Security Hub 콘솔의 요약 대시보드에는 보안 위젯 전반의 노출, 위협, 리소스 및 보안 범위에 대한 개요가 표시됩니다. 위젯을 추가 및 제거하고 필터 세트를 생성 및 적용하여 각 위젯의 데이터를 검색하여 대시보드를 사용자 지정할 수 있습니다.

## 고려 사항

대시보드와 상호 작용하기 전에 다음 사항을 고려하세요.

- 저장된 필터 세트 또는 위젯 레이아웃 변경과 같은 사용자 지정은 자동으로 저장됩니다.
- 대시보드를 열 때마다 데이터가 자동으로 새로 고쳐집니다.
- 교차 리전 집계를 구성하면 대시보드에 연결된 모든 리전의 조사 결과가 포함됩니다(홈 리전에서 대시보드를 볼 때).

계정이 조직의 위임된 관리자 계정, 조직의 멤버 계정 또는 독립 실행형 계정인 경우 다음을 고려하세요.

- 위임된 관리자 계정의 사용자 지정은 멤버 계정의 사용자 지정과 독립적으로 저장됩니다. 사용자 지정에는 저장된 필터 세트 또는 위젯 레이아웃 변경 사항이 포함될 수 있습니다.
- 조직의 위임된 관리자 계정인 경우, 데이터에는 관리자 계정 및 멤버 계정에 대한 조사 결과가 포함됩니다.
- 계정이 조직의 멤버 계정이거나 독립 실행형 계정인 경우 데이터에는 계정에 대한 조사 결과만 포함됩니다.

가장 좋은 방법은 저장된 필터 세트, 사용자 지정 위젯 또는 기타 관련 자유 형식 텍스트 필드에 기밀, 민감한 또는 개인 식별 정보(PII)를 포함하지 않는 것입니다.

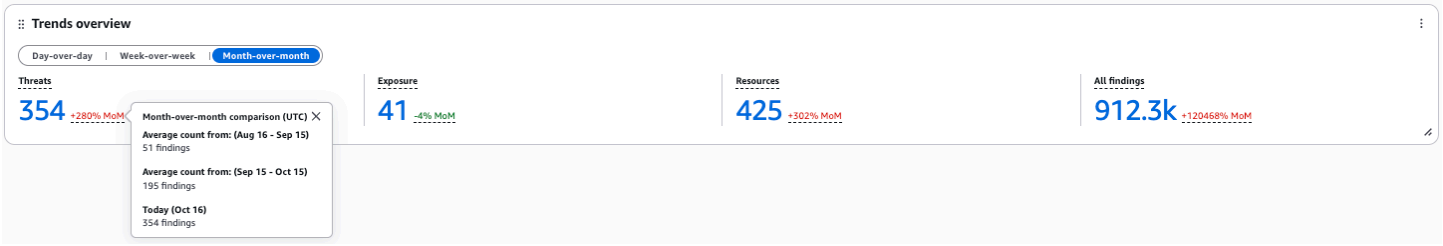
## 사용 가능한 위젯

요약 대시보드의 실행 및 분류 탭에서 다양한 위젯과 상호 작용할 수 있습니다. 경영진 탭에는 노출, 위협 및 리소스에 대한 추세 데이터를 표시하는 위젯과 다양한 보안 기능에서 계정 적용 범위를 추적하는 데 도움이 되는 보안 적용 범위 위젯이 포함되어 있습니다. 분류 탭에는 노출, 위협 및 리소스에 대한 요약을 표시하는 위젯이 포함되어 있습니다. 그러나 두 탭 모두에서 위젯을 추가하고 위젯을 제거하고 각 위젯의 위치를 관리하여 경험을 사용자 지정할 수 있습니다.

### 추세 위젯

다음 위젯은 노출, 위협 및 리소스에 대한 추세 데이터를 표시하므로 시간 경과에 따라 분석할 수 있습니다.

추세 개요 위젯



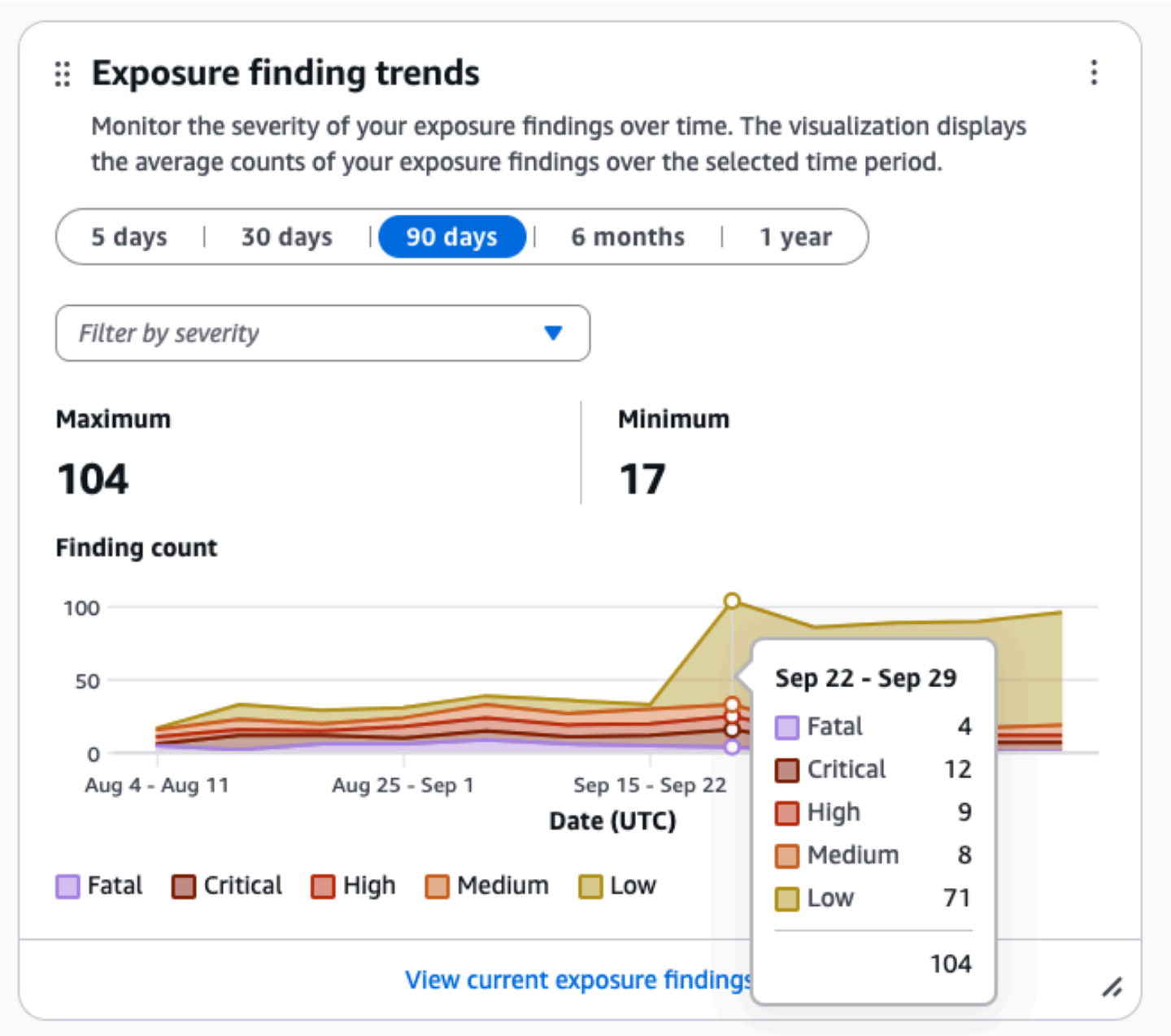

이 위젯은 다음 기간의 노출, 위협, 리소스 및 결과에 대한 개요를 표시합니다.

- Month-over-month 지난 2개월 동안의 period-over-period 개수가 반영됩니다.
- Week-over-week 지난 2주 동안의 period-over-period 개수가 반영됩니다.
- Day-over-day 지난 2일 동안의 period-over-period 개수가 반영됩니다.

백분율 옆의 숫자는 현재까지period-over-period 수를 반영합니다. 이 숫자를 선택하면 콘솔에서 해당 대시보드로 이동합니다. 추세 데이터를 표시하는 다른 대시보드로 이동하면 대시보드는 지난 90일 동안의 추세 데이터만 표시하거나 계정에 30일보다 오래된 결과 또는 리소스가 없는 경우 가장 적합한 기간 동안의 추세 데이터만 표시합니다.

> **Note**
>
> 이 위젯에서 데이터를 수신하려면 다음 보안 서비스를 활성화해야 합니다.
>
> - AWS Security Hub CSPM - 노출에 대한 데이터 수신
> - Amazon Inspector - 노출에 대한 데이터 수신
> - GuardDuty - 위협에 대한 데이터 수신

노출 조사 결과 추세 위젯




이 위젯은 다음 기간에 노출 결과의 심각도를 표시합니다.

- 5일
- 30일
- 90일
- 6개월
- 1년

시각화에는 선택한 기간 동안의 평균 조사 결과 수가 표시됩니다.

심각도 필터

다음 심각도 필터를 포함하거나 제외하여 그래프를 업데이트할 수 있습니다.

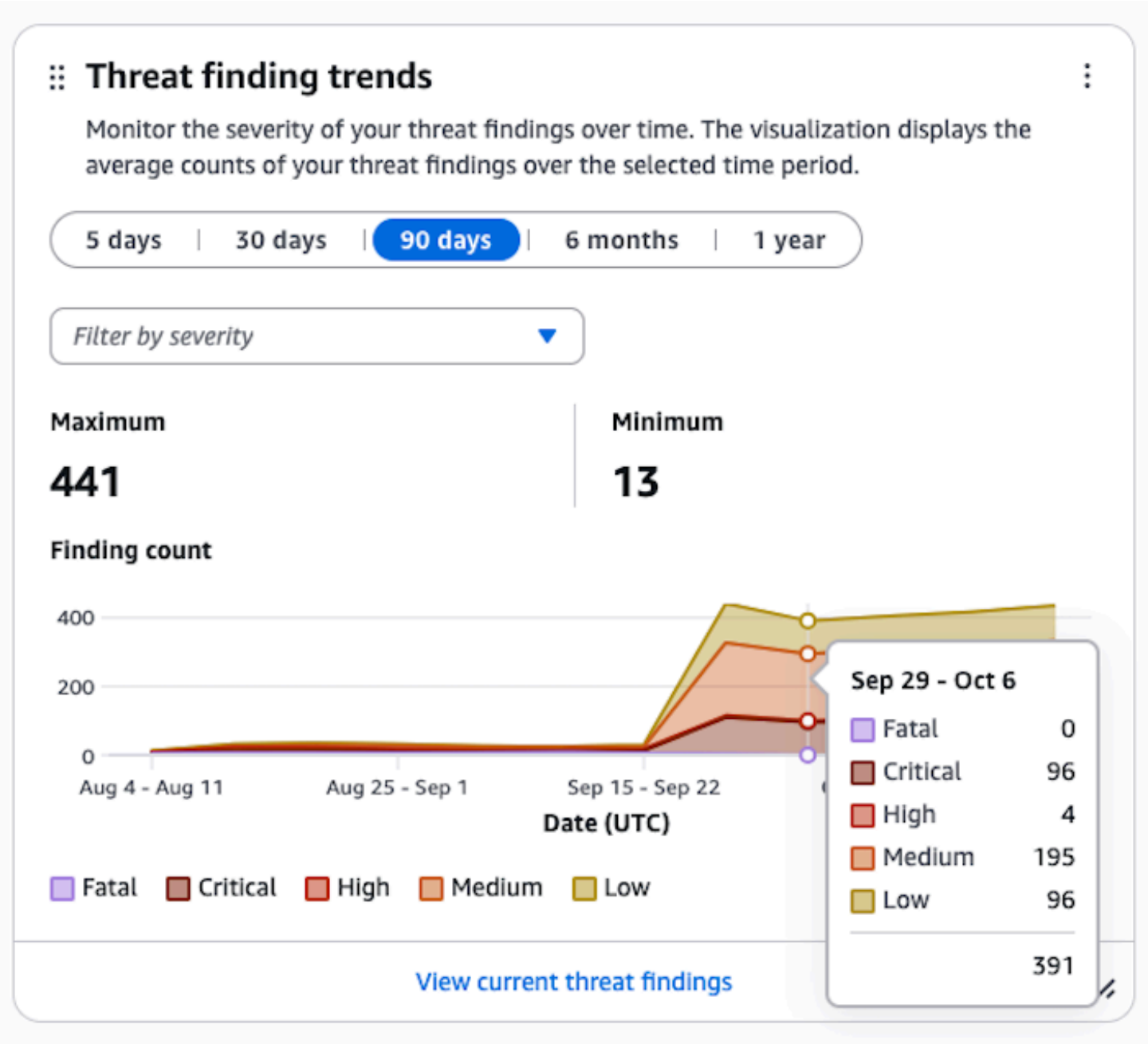
- 치명적
- 위험
- 높음
- 중간
- 낮음
- 정보 제공
- 기타
- 알 수 없음

적용된 심각도 필터는 시각화 하단에 서로 다른 상자로 표시됩니다. 시각화 위로 마우스를 가져가 특정 시점의 평균 조사 결과 수를 검토할 수 있습니다. 적용된 각 심각도 필터와 일치하는 결과의 평균 수를 검토할 수도 있습니다.

모든 현재 노출 결과 보기를 선택하여 노출 대시보드로 이동할 수 있습니다. 기본적으로 노출 대시보드에는 지난 90일 동안의 추세 데이터만 표시됩니다. 계정에 30일이 지난 노출 조사 결과가 포함되어 있지 않은 경우 대시보드는 최적의 기간을 기준으로 추세 데이터를 표시합니다.

> **Note**
>
> 이 위젯에서 데이터를 수신하려면 Amazon Inspector 및 Security Hub CSPM을 활성화해야 합니다.

위협 조사 결과 추세 위젯




이 위젯은 다음 기간에 위협 조사 결과의 심각도를 표시합니다.

- 5일
- 30일
- 90일
- 6개월
- 1년

시각화에는 선택한 기간 동안의 평균 조사 결과 수가 표시됩니다.

심각도 필터

다음 심각도 필터를 포함하거나 제외하여 그래프를 업데이트할 수 있습니다.

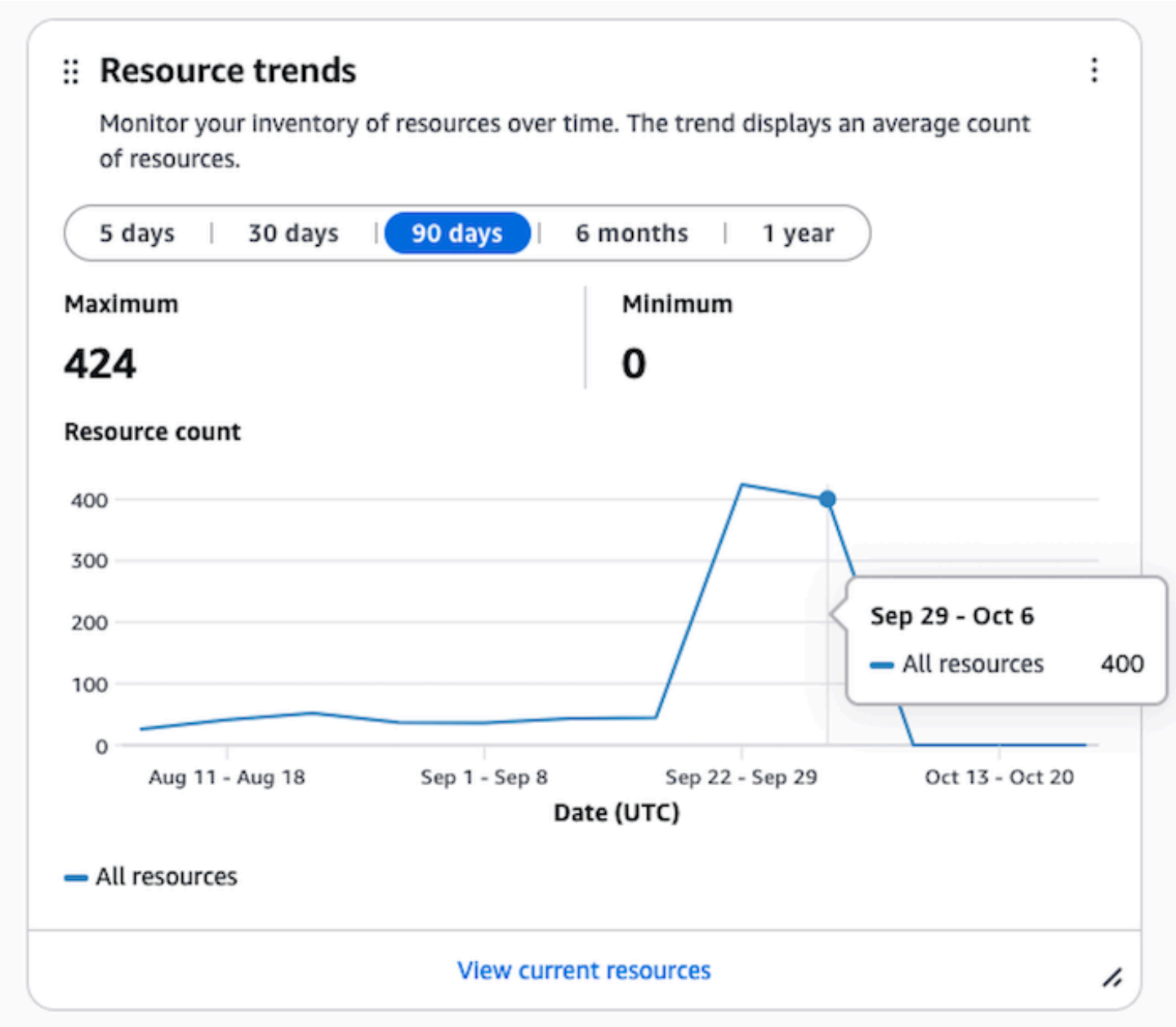
- 치명적
- 위험
- 높음
- 중간
- 낮음
- 정보 제공
- 기타
- 알 수 없음

적용된 심각도 필터는 시각화 하단에 서로 다른 상자로 표시됩니다. 시각화 위로 마우스를 가져가 특정 시점의 평균 조사 결과 수를 검토할 수 있습니다. 적용된 각 심각도 필터와 일치하는 결과의 평균 수를 검토할 수도 있습니다.

모든 현재 위협 조사 결과 보기를 선택하여 노출 대시보드로 이동할 수 있습니다. 기본적으로 위협 대시보드에는 지난 90일 동안의 추세 데이터만 표시됩니다. 계정에 30일이 지난 위협 조사 결과가 포함되어 있지 않은 경우 대시보드는 최적의 기간을 기준으로 추세 데이터를 표시합니다.

> **Note**
>
> 이 위젯에서 데이터를 수신하려면 GuardDuty를 활성화해야 합니다.

## 리소스 추세 위젯




이 위젯은 다음 기간의 리소스 인벤토리를 표시합니다.

- 5일
- 30일
- 90일
- 6개월
- 1년

시각화에는 선택한 기간 동안의 평균 리소스 수가 표시됩니다. 시각화 위로 마우스를 가져가 특정 시점의 평균 리소스 수를 검토할 수 있습니다.

현재 리소스 보기를 선택하여 리소스 대시보드로 이동할 수 있습니다. 기본적으로 리소스 대시보드에는 지난 90일 동안의 추세 데이터만 표시됩니다. 계정에 30일보다 오래된 리소스가 없는 경우 대시보드는 최적의 기간을 기준으로 추세 데이터를 표시합니다.

이 위젯은 다음 기간의 리소스 인벤토리를 표시합니다.

- 5일
- 30일
- 90일
- 6개월
- 1년

추세에 대한 데이터 보존

Security Hub는 Security Hub가 활성화된 모든 AWS 계정 에 대해 추세 데이터를 1년 동안 유지합니다. 추세 데이터가 1년 동안 보존되면 Security Hub에서 삭제됩니다.

Security Hub가 비활성화된 후 또는 계정이 종료된 경우 위임된 관리자 및 독립 실행형 계정에 대한 추세 데이터가 삭제됩니다.

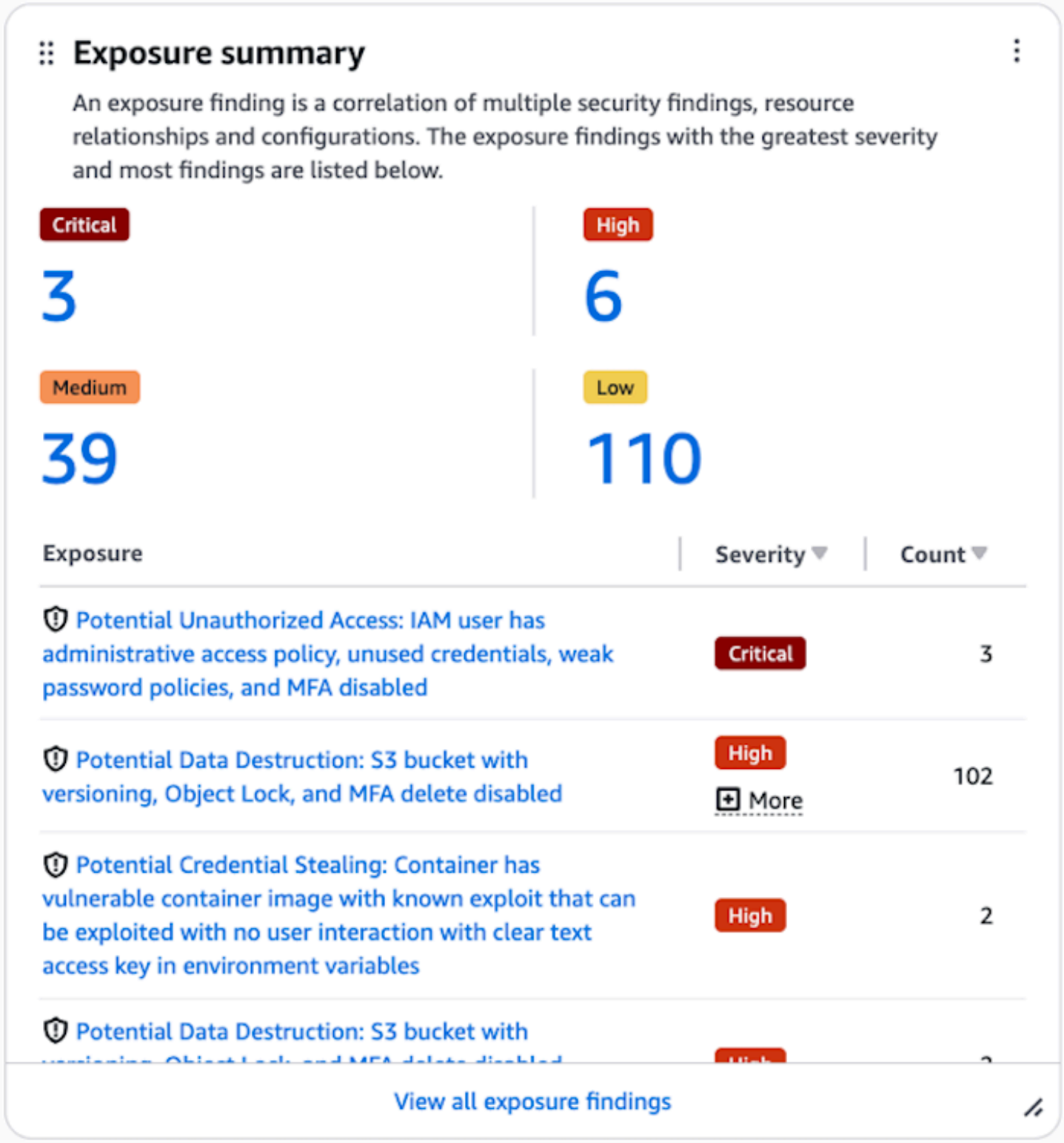
Security Hub가 활성화된 멤버 계정에 대한 추세 데이터 보존 시나리오:

- 멤버 계정이 조직을 떠나도 Security Hub는 계정이 조직을 떠난 시점까지 1년 동안 추세 데이터를 계속 저장합니다.
- 멤버 계정에 대해 Security Hub가 비활성화된 경우 Security Hub는 계정이 비활성화된 시점까지 1년 동안 추세 데이터를 유지합니다.
- 멤버 계정이 종료되면 Security Hub는 종료된 계정에서 추세 데이터를 연결 해제하고(예: 종료된 계정 ID 스크러빙) 나머지 추세 데이터를 1년 동안 유지합니다.

## 요약 위젯

다음 위젯에는 노출, 위협 및 리소스에 대한 요약이 표시됩니다.

노출 요약 위젯

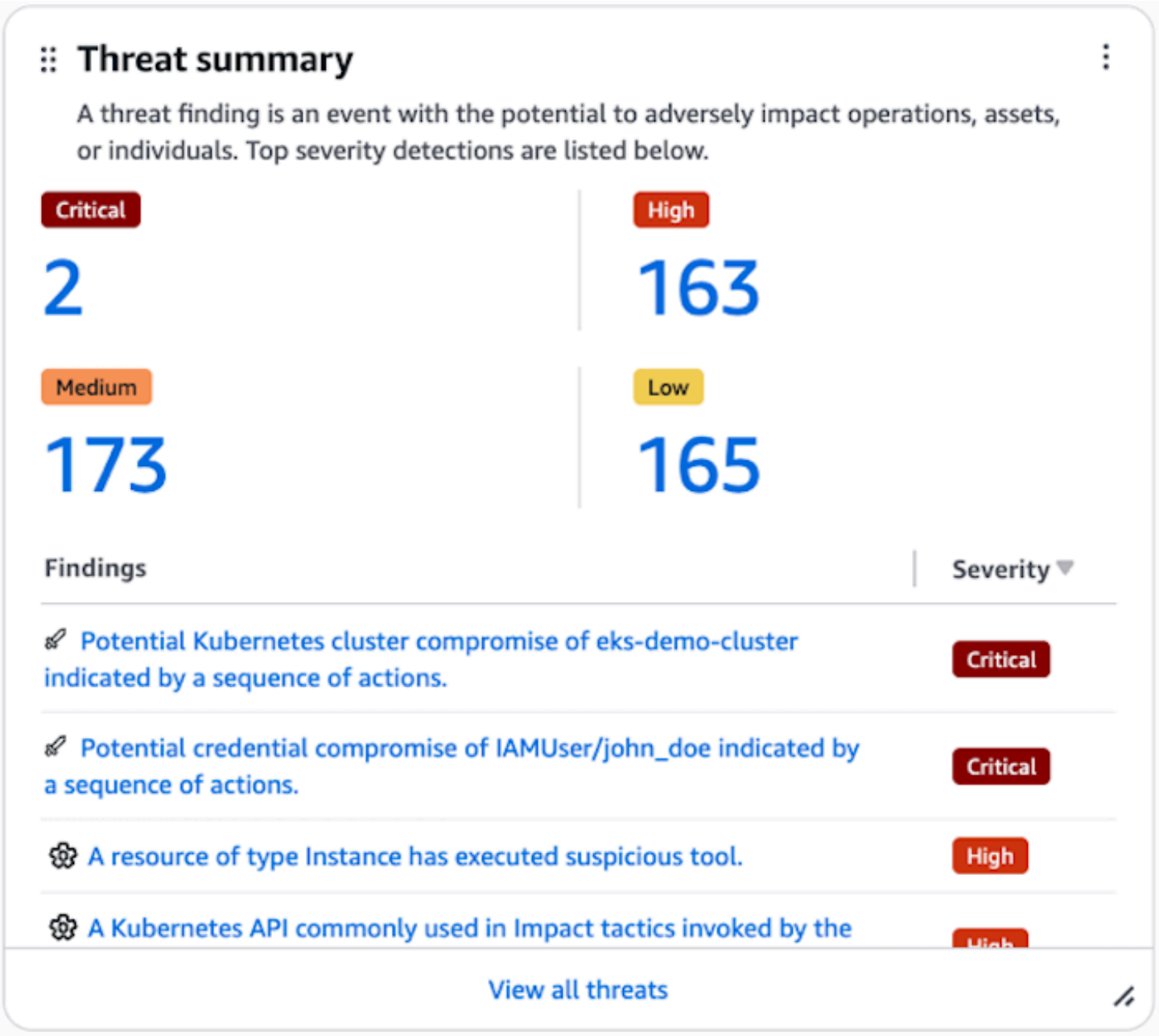



이 위젯은 심각도별로 노출을 표시합니다. 노출은 Security Hub 및 Amazon Inspector와 같은 기타 AWS 보안 서비스의 조사 결과 및 특성에 대한 분석을 기반으로 합니다. 이 위젯의 노출 목록은 심각도

가 가장 높은 8개 노출로 제한됩니다. 심각도가 더 높은 노출이 목록에서 먼저 나타납니다. 두 개 이상의 노출의 심각도가 같으면 목록은 해당 노출을 최근 노출보다 자동으로 그룹화합니다. 모든 노출 보기를 선택하면 노출 대시보드로 이동합니다.

> **Note**
>
> 이 위젯의 데이터를 수신하려면 Amazon Inspector 및 Security Hub CSPM을 활성화해야 합니다.

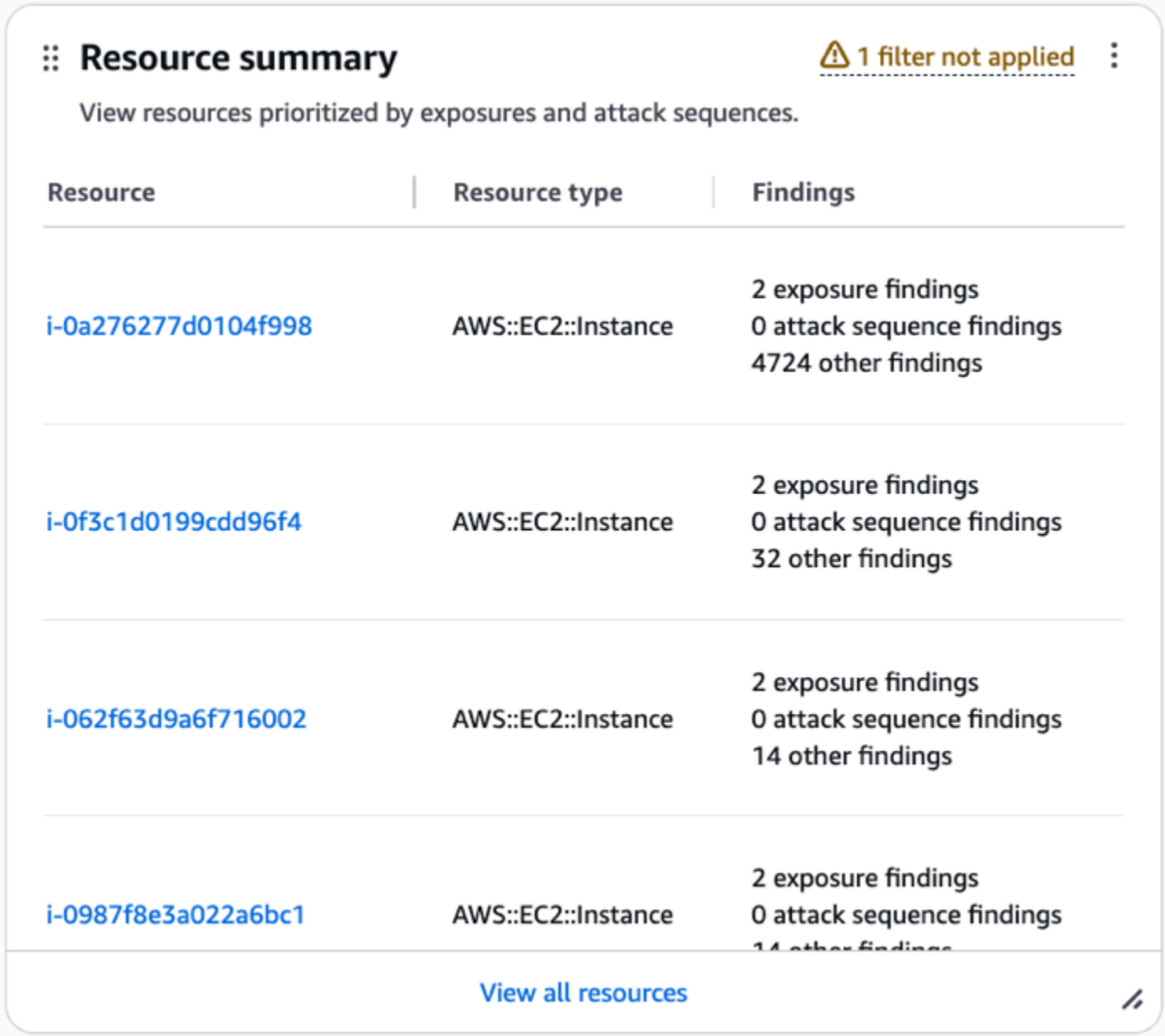
위협 요약 위젯




이 위젯은 심각도별로 위협을 표시합니다. 위협은 환경의 보안을 손상시킬 수 있는 악의적인 활동 또는 의심스러운 활동을 말합니다. 이 위젯의 위협 목록은 심각도가 가장 높은 8개 위협으로 제한됩니다. 심각도가 더 높은 위협은 목록에서 먼저 나타납니다. 둘 이상의 위협의 심각도가 동일한 경우 목록은 해당 위협을 최신 위협에 자동으로 그룹화합니다. 모든 위협 보기를 선택하면 위협 대시보드로 이동합니다.

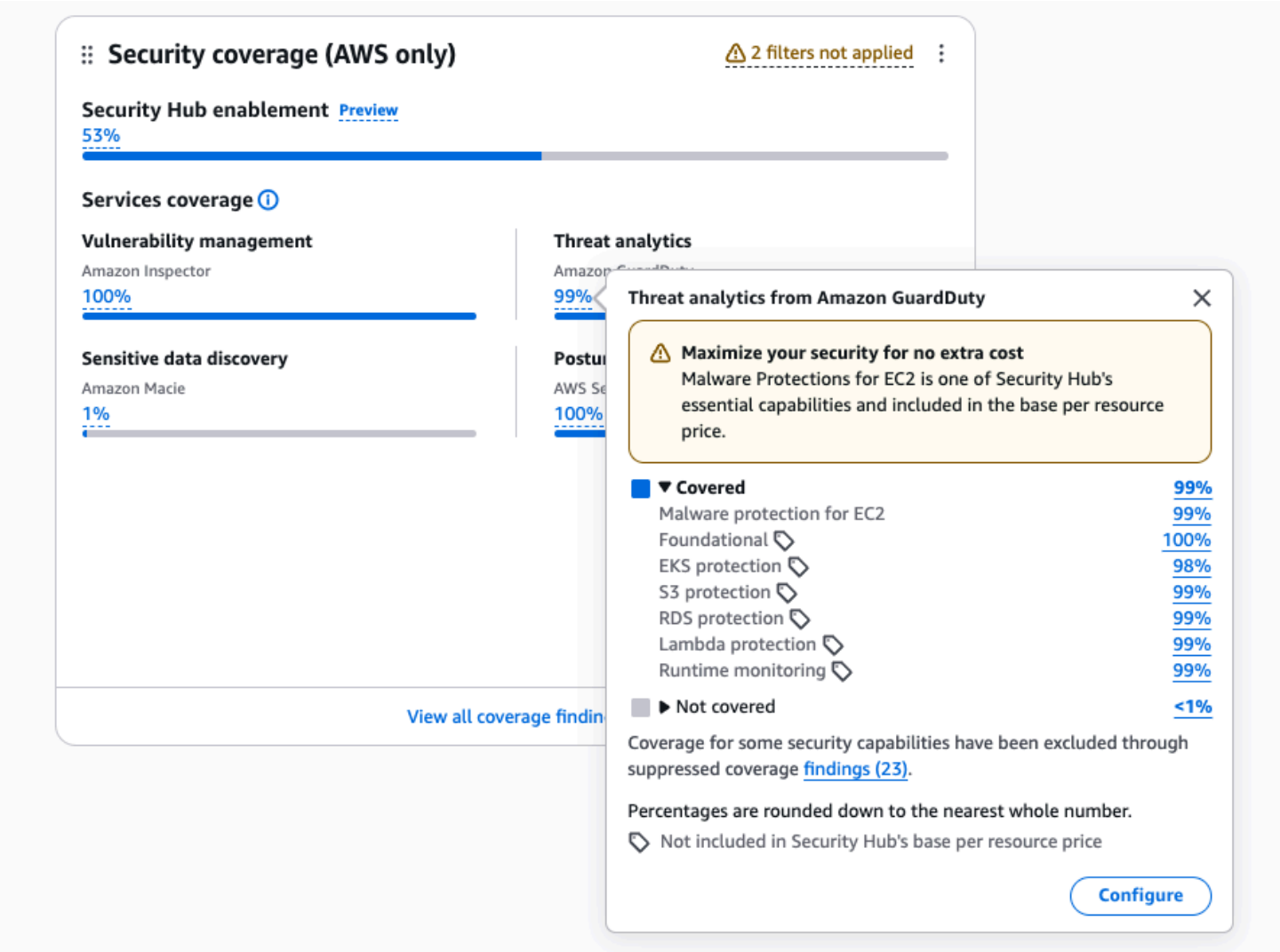
> **Note**
>
> 이 위젯에서 데이터를 수신하려면 GuardDuty를 활성화해야 합니다.

리소스 요약 위젯




이 위젯은 리소스 유형 및 리소스와 관련된 조사 결과를 기준으로 리소스를 표시합니다. 리소스는 노출 및 공격 시퀀스에 따라 우선순위가 지정됩니다. 모든 리소스 보기를 선택하면 리소스 대시보드로 이동합니다.

## 보안 적용 범위 위젯




위젯에는 다음 보안 기능에 대한 계정 적용 범위 요약이 표시됩니다.

- Amazon Inspector의 취약성 관리
- Amazon GuardDuty의 위협 탐지
- Amazon Macie의 민감한 데이터 검색
- AWS Security Hub CSPM의 태세 관리

위임된 관리자 계정에서 위젯은 Security Hub 활성화에 대한 계정 적용 범위도 표시합니다.

각 적용 범위 항목은 계정 전체에서 해당 기능의 활성화를 나타내는 백분율을 표시합니다. 백분율을 선택하면 해당 기능의 적용 범위에 대한 세부 정보가 표시됩니다. Security Hub 활성화 비율을 선택하면 측면 패널이 표시됩니다. 패널에는 조직 전체의 각 리전에서 활성화된 계정 수가 표시됩니다.

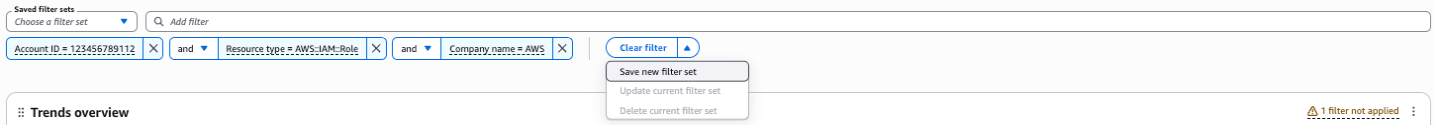
서비스 적용 범위 섹션에서 백분율은 각 보안 기능에 대해 통과한 적용 범위 검사의 비율을 나타냅니다. 이러한 검사는 Security Hub가 활성화된 계정 및 리전에 적용됩니다. 적용 범위 백분율을 선택하면 각 기능을 적용됨(확인 통과) 또는 적용되지 않음(확인 실패)으로 분류하는 팝오버가 표시됩니다. 백분율은 가장 가까운 정수로 내림됩니다. 팝오버에서 백분율을 선택하면 해당 백분율을 구성하는 결과에 대한 세부 정보가 포함된 적용 범위 조사 결과 페이지가 열립니다. 구성을 선택하여 해당 기능에 대한 구성을 관리할 수 있는 개별 서비스를 열거나 보안 서비스에 대한 구성을 업데이트할 수 있는 Security Hub 구성 페이지를 엽니다.

Security Hub에서 적용 범위 조사 결과가 표시되지 않으면 위젯에 적용 범위가 제외되었음을 알리는 메시지가 표시됩니다. 억제된 적용 범위 조사 결과를 통해 보안 기능에 대한 적용 범위가 제외되었습니다.

적용 범위 조사 결과를 보고 억제하는 방법에 대한 자세한 내용은 Security Hub의 적용 범위 조사 결과를 참조하세요.

## 사용 가능한 필터

필터 추가 막대를 사용하여 보안 위젯에 필터를 적용할 수 있습니다.




필터는 다음 범주로 구성됩니다.

- 공유 필터 - 모든 보안 위젯에 적용
- 결과 필터 - 결과 데이터를 표시하는 보안 위젯에 적용됩니다.
- 리소스 필터 - 리소스 데이터를 표시하는 보안 위젯에 적용됩니다.

및/또는 연산자를 사용하여 필터를 연결한 다음 드롭다운에서 새 필터 세트 저장을 선택하여 필터 세트를 생성할 수 있습니다.

### 노출 조사 결과 추세 위젯 및 위협 조사 결과 추세 위젯에 적용된 필터

현재 이러한 위젯에 지원되는 필터에는 다음이 포함됩니다.

- 계정 ID
- 검색 클래스 이름
- 찾기 유형

- 제품 이름
- 리전
- 상태

### 리소스 추세 위젯에 적용된 필터

현재이 위젯에 지원되는 필터에는 다음이 포함됩니다.

- 계정 ID
- 리전
- 리소스 범주
- 리소스 유형

### 위젯에 적용되지 않는 필터




위젯이 필터를 지원하지 않는 경우 필터는 위젯에 적용되지 않습니다. 이 경우 위젯은 적용되지 않은 필터 수를 알려주는 경고 메시지를 표시하고 지원하지 않는 필터의 이름을 나열합니다.

## Security Hub에서 리소스 세부 정보 보기

리소스 페이지는 계정 및 조직 전반의 공통 리소스를 추적합니다. Security Hub 콘솔의 탐색 창에서 리소스를 선택하여 리소스 페이지에 액세스할 수 있습니다. 리소스 페이지의 이점은 보안 태세를 모니터링하고, 리소스를 구성하고, 리소스 세부 정보를 검토하는 데 도움이 된다는 것입니다. 리소스 유형을 선택하면 리소스 유형과 연결된 모든 리소스를 검토할 수 있습니다. 리소스와 연결된 모든 조사 결과를 검토할 수 있습니다. 리소스 페이지에서 사용할 수 있는 리소스 유형에는 Security Hub에 조사 결과를 제공하는 AWS 보안 서비스가 적용되는 계정의 모든 리소스가 포함됩니다.

> **Note**
>
> 위임된 관리자는 멤버 계정과 연결된 모든 리소스를 볼 수 있습니다. 홈을 구성한 경우 홈의 모든 리소스를 연결된 AWS 리전 에서 볼 AWS 리전수 있습니다 AWS 리전.

리소스를 선택하면 해당 리소스의 세부 정보를 검토할 수 있습니다. 이러한 세부 정보에는 리소스 이름, ID, ARN, 유형, 범주가 포함됩니다. 리소스와 연결된 계정 ID, 리소스가 생성된 시간(타임스탬프), 리소스가 생성된 위치(AWS 리전)를 검토할 수 있습니다. 리소스에 대한 추가 구성 세부 정보도 검토할 수 있습니다. 이러한 세부 정보는 복사할 수 있는 JSON 코드 조각에서 찾을 수 있습니다.

개요 탭에서 조사 결과 탭으로 전환하면 해당 리소스와 연결된 모든 조사 결과를 검토할 수 있습니다. 조사 결과 탭에는 각 조사 결과의 이름, 각 조사 결과의 유형, 각 조사 결과의 심각도가 표시됩니다. 여러 필드를 기준으로 조사 결과를 그룹화하고 필터를 사용하여 조사 결과를 검색할 수 있습니다. 조사 결과를 선택하면 조사 결과의 개요를 검토할 수 있습니다. 여기에는 규정 준수에 관한 정보, 조사 결과와 관련된 문제를 해결하는 방법이 포함됩니다. 특성 탭에는 리소스에 대해 식별된 각 특성이 표시됩니다. 리소스에 대한 노출 조사 결과를 생성하는 데 사용된 기여 특성을 볼 수 있습니다. 리소스에 대해 식별되었지만 노출 조사 결과에 직접 기여하지 않은 다른 보안 항목인 컨텍스트 특성도 볼 수 있습니다. 리소스로 돌아가 리소스 열기를 선택하면 리소스 유형별 콘솔에서 리소스를 검토할 수 있습니다. 예를 들어 리소스가 IAM 리소스인 경우 IAM 콘솔에서 리소스를 열 수 있습니다.

리소스 페이지에서는 리소스를 구성하고 검색하는 다양한 방법을 제공합니다. 리소스를 유형별로 그룹화할 수 있습니다. 예를 들어 계정 ID, 결과 유형, 리소스 범주 AWS 리전, 리소스 이름 및 리소스 유형별로 리소스를 그룹화할 수 있습니다. 빠른 필터를 사용하면 범주, 계정 및 조사 결과 유형별로 리소스를 검토할 수 있습니다.

# Security Hub 및 Open Cybersecurity Schema Framework(OCSF)

Security Hub는 Open Cybersecurity Schema Framework(OCSF)를 모든 보안 조사 결과의 표준 형식으로 사용합니다. 이 주제에서는 OCSF와 Security Hub가 이를 구현하는 방법을 설명합니다.

## OCSF 개요

Security Hub 조사 결과는 OCSF(Open Cybersecurity Schema Framework)를 사용하여 형식이 지정됩니다. OCSF는 공급업체에 구애받지 않는 코어 보안 스키마와 함께 스키마 개발을 위한 확장 가능한 프레임워크를 제공하는 오픈 소스 프로젝트입니다. 공급업체 및 기타 데이터 생산자는 특정 도메인에 맞게 스키마를 채택하고 확장할 수 있습니다. 데이터 생산자는 다양한 스키마를 매핑하여 보안 팀이 데이터 수집 및 정규화를 간소화하여 데이터 과학자와 분석가가 위협 탐지 및 조사를 위해 공통 언어로 작업할 수 있도록 지원할 수 있습니다. 목표는 기존 보안 표준 및 프로세스를 보완하는 동시에 모든 환경, 애플리케이션 또는 솔루션에 채택되는 개방형 표준을 제공하는 것입니다.

프레임워크는 데이터 유형, 속성 사전 및 분류로 구성됩니다. 사이버 보안 또는 이벤트에 국한되지는 않지만, 처음에는 사이버 보안 이벤트 스키마에 중점을 둡니다. OCSF는 스토리지 형식, 데이터 수집 방법 및 ETL 프로세스와 무관합니다.

Security Hub는 현재 OCSF 스키마 버전 1.6의 결과를 지원합니다.

## 관련 리소스

OCSF 및 해당 구현에 대한 자세한 내용은 다음 리소스를 참조하세요.

- 퍼블릭 OCSF 설명서
- OCSF 확장 사용 설명서
- OCSF 코어 스키마 참조
- OCSF 확장 레지스트리

## AWS OCSF 확장

OCSF 스키마는 새 속성, 객체, 범주, 프로필 및 이벤트 클래스를 추가하여 확장할 수 있습니다. 스키마는 코어 스키마 엔터티 및 확장의 집계입니다.

OCSF 확장을 통해 특정 공급업체 또는 고객은 속성을 추가하여 도메인별 사용자 지정을 제공하고, 데이터 상호 운용성을 개선하고, 보안 분석을 위한 보다 상세한 컨텍스트를 추가하여 기존 스키마를 보강할 수 있습니다.

OCSF( AWS Extension for Open Cybersecurity Schema Framework)는 OCSF 이벤트 내의 클라우드 리소스에 대한 속성 정의를 제공합니다. 이 확장은 클라우드별 리소스 속성을 사용하여 OCSF `resource_details` 객체를 확장하는 `cloud_resources` 프로파일을 추가합니다. 보안 팀은 이러한 속성을 사용하여 리소스 구성, 잠재적 취약성 및 위협 탐지 메타데이터를 분석할 수 있습니다.

### 확장 **`resource_details`** 객체

AWS 확장은 아래 속성 참조 목록에 언급된 속성으로 `resource_details` 객체를 확장합니다. 이러한 속성은 표준화된 이벤트 프레임워크 내에서 다양한 공급자에 걸쳐 클라우드 리소스를 적절하게 식별하고 분류할 수 있도록 합니다.

### AWS OCSF 속성 참조의 확장

기본 속성 및 리소스별 객체 섹션에서는 resource_details에 대한 AWS OCSF 확장의 일부인 각 속성의 예를 제공합니다.

각 속성 정의에는 퍼블릭 OCSF 스키마와의 현재 관계를 설명하는 OCSF 상태가 포함되어 있습니다.

- 기존:이 속성은 이미 표준 OCSF resource_details에 있으며 이제 AWS 확장의 일부입니다.

- 신규: 속성은 OCSF의 일부가 아니며 AWS 확장의 일부로 도입되었습니다. 코어 OCSF 스키마에 존재하지 않습니다.
- resource_details에 추가됨: 속성은 OCSF에 정의되지만 resource_details의 일부는 아닙니다.

## 기본 속성

리소스 식별, 위치 및 기본 메타데이터에 사용되는 기본 속성입니다. 문자열, 타임스탬프 및 배열과 같은 간단한 데이터 유형으로 구성됩니다.

클라우드 파티션

리소스가 있는 클라우드 파티션입니다.

요구 사항

권장

유형

문자열

OCSF 상태

기존

예제

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

소유자 계정 ID

리소스가 속한 12자리 계정 식별자입니다.

요구 사항

권장

유형

문자열

OCSF 상태

기존

예제

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

리소스 유형

특정 서비스 및 리소스를 식별하는 AWS CloudFormation 리소스 유형입니다.

요구 사항

필수

유형

문자열

형식

AWS CloudFormation 리소스 유형 명명 규칙을 따라야 합니다.
`AWS::<Service>::<ResourceType>`

OCSF 상태

기존

예제

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

리소스 식별자

클라우드 리소스의 고유 식별자(예: i-1234567890abcdef0).

요구 사항

권장

유형

문자열

형식

유효한 리소스 식별자여야 합니다. 최소 길이는 1이고, 최대 길이는 768입니다.

OCSF 상태

기존

예제

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

대체 리소스 식별자

클라우드 리소스의 고유 식별자로, 일반적으로 Amazon 리소스 이름(ARN)입니다.

요구 사항

권장

유형

문자열

형식

유효한 AWS ARN이어야 합니다. 일반적인 패턴은 다음과 같습니다.

- `"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"`

참고: S3와 같은 일부 서비스는 arn:aws:s3:::bucket-name(리전 또는 계정 ID 제외)과 같은 변형을 사용합니다.

OCSF 상태

기존

예시

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

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

리소스 이름

클라우드 리소스의 고유한 이름입니다.

요구 사항

권장

유형

문자열

형식

값이 환경에 따라 달라지는 사용자 생성 이름입니다.

OCSF 상태

기존

예제

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

클라우드 리전

리소스가 위치한 AWS 리전입니다.

요구 사항

권장

유형

문자열

형식

유효한 클라우드 리전 식별자(예: us-east-1, eu-west-1, ap-southeast-2)

OCSF 상태

기존

예제

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

리소스 생성 시간

리소스가 생성된 시간입니다.

요구 사항

권장

유형

타임스탬프

형식

epoch 이후 밀리초 단위의 Unix 타임스탬프(1970년 1월 1일, 00:00:00 UTC)

OCSF 상태

기존

예제

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

Tags

리소스 메타데이터 및 조직에 대한 키-값 페어입니다.

요구 사항

권장

유형

키:값 객체 배열

형식

가 키:값 페어를 정의할 수 있는 일반 객체입니다.

OCSF 상태

기존

예제

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

IP 주소

IPv4 또는 IPv6 형식의 인스턴스와 연결된 IP 주소입니다.

요구 사항

선택 사항

유형

문자열

형식

유효한 IPv4 또는 IPv6 주소

OCSF 상태

기존

예제

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

IP 주소

디바이스와 연결된 IP 주소(IPv4 또는 IPv6)의 배열입니다. 여기에는 퍼블릭 및 프라이빗 IP 주소가 모두 포함될 수 있습니다.

요구 사항

선택 사항

유형

IP 주소 배열

OCSF 상태

New

예제

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

```
  ]
}
```

### VPC UID

리소스가 위치한 VPC ID입니다.

요구 사항

선택 사항

유형

문자열

형식

VPC 식별자(예: vpc-12345678900)

OCSF 상태

에 추가됨 `resource_details`

예제

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

기본 속성이 있는 리소스 객체 예제

```
{
  "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"
    }
  ]
}
```

## 리소스별 객체

이는 특정 리소스 유형 및 서비스에 대한 자세한 정보를 제공하는 복잡한 중첩 객체입니다. 각 객체에는 서비스별 구성 및 메타데이터가 있는 여러 필드와 하위 객체가 포함되어 있습니다.

장치

암호화 세부 정보, 이미지 정보, 인스턴스 프로파일 및 시작 시간을 포함하여 컴퓨팅 리소스에 대한 클라우드 인스턴스 속성이 향상되었습니다.

요구 사항

선택 사항

유형

객체

OCSF 상태

에가 추가되었습니다`resource_details`. OCSF 디바이스 객체 정의를 참조하세요.

AWS 확장은이 객체에 다음 속성을 추가합니다.

- `encryption_details` - 리소스의 암호화 세부 정보
- `image` - 이미지 정보
- `instance_profile` - 인스턴스와 연결할 IAM 인스턴스 프로파일
- `launch_time` - 인스턴스가 시작된 시간

- `uid_alt` - 리소스의 Amazon 리소스 이름(ARN)

예제

```
{
  "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"
  }
}
```

네트워크 인터페이스

연결 및 보안 그룹을 포함한 네트워크 인터페이스 세부 정보 및 구성입니다.

요구 사항

선택 사항

유형

객체

OCSF 상태

에가 추가되었습니다`resource_details`. OCSF 네트워크 인터페이스 객체 정의를 참조하세요.

AWS 확장은이 객체에 다음 속성을 추가합니다.

- `attachments` - 네트워크 인터페이스 연결에 대한 정보
- `security_groups` - 보안 그룹 고유 식별자 배열
- `uid_alt` - 리소스의 Amazon 리소스 이름(ARN)

예제

```
{
  "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"
      }
    ]
  }
```

```
}
```

스토리지 디바이스

첨부 파일, 암호화 및 스냅샷 정보를 포함한 스토리지 디바이스 세부 정보입니다.

요구 사항

선택 사항

유형

객체

OCSF 상태

New

스토리지 디바이스 객체에는 다음 속성이 포함됩니다.

- `name` - 스토리지 디바이스의 이름
- `uid` - 스토리지 디바이스의 고유 식별자
- `attachments` - 스토리지 디바이스 연결
- `encryption_details` - 스토리지 디바이스 암호화 키
- `is_encrypted` - 스토리지 디바이스 암호화 여부(필수)
- `snapshot_id` - 스토리지 디바이스 스냅샷 식별자
- `uid_alt` - 리소스의 Amazon 리소스 이름(ARN)

예제

```
{
  "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"
  }
```

```
}
```

Database

엔진 유형, 엔드포인트 및 사용자 정보를 포함한 데이터베이스 인스턴스 속성.

요구 사항

선택 사항

유형

객체

OCSF 상태

에가 추가되었습니다`resource_details`. OCSF 데이터베이스 객체 정의를 참조하세요.

AWS 확장은이 객체에 다음 속성을 추가합니다.

- `cluster_uid` - 데이터베이스 클러스터 식별자
- `db_endpoint` - 데이터베이스 엔드포인트
- `encryption_details` - 데이터베이스 암호화 세부 정보
- `engine` - 데이터베이스 엔진 이름(예: mysql)
- `is_encrypted` - 데이터베이스 암호화 여부
- `is_iam_authentication` - IAM 인증 활성화 여부
- `is_public` - 데이터베이스에 공개적으로 액세스할 수 있는지 여부
- `port` - 데이터베이스 포트 번호
- `security_groups` - 데이터베이스 인스턴스와 연결된 VPC 보안 그룹 배열
- `snapshot_details` - 데이터베이스 스냅샷 세부 정보
- `status` - 데이터베이스 상태(예: 사용 가능)
- `subnet_group` - 데이터베이스 서브넷 그룹은 VPC의 서브넷 모음입니다.
- `uid_alt` - 리소스의 Amazon 리소스 이름(ARN)
- `user` - 데이터베이스 사용자
- `version` - 데이터베이스 버전

예제

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

데이터베이스 클러스터

엔진 유형, 엔드포인트 및 사용자 정보를 포함한 데이터베이스 인스턴스 속성.

요구 사항

선택 사항

유형

객체

OCSF 상태

New

데이터베이스 객체에는 다음 속성이 포함됩니다.

- `uid` - 데이터베이스 클러스터의 고유 식별자
- `uid_alt` - 리소스의 Amazon 리소스 이름(ARN)
- `name` - 데이터베이스 클러스터의 이름
- `status` - 데이터베이스 클러스터 상태
- `engine` - 클러스터와 연결된 엔진
- `version` - 데이터베이스 클러스터 버전
- `cluster_members` - 클러스터의 일부인 데이터베이스 인스턴스 목록

- security_groups - 클러스터와 연결된 보안 그룹 배열
- is_encrypted - 데이터베이스 클러스터 암호화 여부
- is_iam_authentication - IAM 인증 활성화 여부
- encryption_details - 데이터베이스 클러스터 암호화 세부 정보
- subnet_group - 클러스터와 연결된 서브넷 그룹
- port - 데이터베이스 클러스터 포트 번호
- zones - 가용 영역 목록
- db_endpoint - 데이터베이스 클러스터 엔드포인트
- snapshot_details - 데이터베이스 스냅샷의 세부 정보

예제

```
{
  "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
    }
  }
}
```

클라우드 함수

핸들러, 계층 및 런타임 구성을 포함한 서버리스 함수의 클라우드 함수 속성입니다.

요구 사항

선택 사항

유형

객체

OCSF 상태

New

클라우드 함수 객체에는 다음 속성이 포함됩니다.

- `name` - 클라우드 함수의 이름
- `uid` - 클라우드 함수의 고유 식별자
- `uid_alt` - 리소스의 Amazon 리소스 이름(ARN)
- `encryption_details` - 클라우드 함수 암호화 세부 정보
- `handler` - 이벤트를 처리하는 함수 코드의 메서드
- `layers` - 보조 코드 또는 데이터가 포함된 클라우드 함수 계층 목록
- `runtime` - 클라우드 함수 언어별 환경
- `security_groups` - 클라우드 함수와 연결된 보안 그룹 배열

- `subnet_info_list` - 클라우드 함수와 연결된 서브넷에 대한 세부 정보
- `user` - 서비스에 액세스할 수 있는 cloud_function 권한을 부여하는 IAM 엔터티에 대한 세부 정보
- `version` - 클라우드 함수 버전
- `vpc_uid` - 클라우드 함수가 VPC에 있는 경우 VPC의 고유 식별자입니다.

예제

```
{
  "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

S3 버킷 또는 데이터 스토리지 속성.

요구 사항

선택 사항

유형

객체

OCSF 상태

에가 추가되었습니다`resource_details`. OCSF Databucket 객체 정의를 참조하세요.

참고:이 객체는 AWS 확장에 의해 resource_details에 추가됩니다. 코어 OCSF Databucket 객체는 추가 속성 없이 사용됩니다.

예제

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

이미지

플랫폼 및 사용 세부 정보를 포함한 컴퓨팅 리소스의 이미지 정보입니다.

요구 사항

선택 사항

유형

객체

OCSF 상태

에가 추가되었습니다`resource_details`. OCSF 이미지 객체 정의를 참조하세요.

AWS 확장은이 객체에 다음 속성을 추가합니다.

- `platform` - 이미지의 운영 체제 플랫폼

- `in_use_count` -이 이미지를 사용하는 리소스 수

예제

```
{
  "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
  }
}
```

서브넷 정보

리소스가 위치한 서브넷에 대한 세부 정보입니다.

요구 사항

선택 사항

유형

객체

OCSF 상태

New

서브넷 정보 객체에는 다음 속성이 포함됩니다.

- `uid` - 서브넷의 고유 식별자입니다.
- `uid_alt` - 리소스의 Amazon 리소스 이름(ARN)
- `name` - 서브넷의 이름
- `zone` - 가용 영역
- `ip_count` - 서브넷의 IP 주소 수
- `cidr_block` - 서브넷의 CIDR 블록
- `is_default` - 기본 서브넷인지 여부

- `is_public` - 서브넷에 공개적으로 액세스할 수 있는지 여부
- `state` - 서브넷의 상태
- `vpc_uid` - 서브넷이 위치한 VPC ID

예제

```
{
  "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"
  }
}
```

User

인스턴스 프로파일 및 정책을 포함한 IAM 사용자 속성.

요구 사항

선택 사항

유형

객체

OCSF 상태

에가 추가되었습니다`resource_details`. OCSF 사용자 객체 정의를 참조하세요.

사용자 객체에는 다음 속성이 포함됩니다.

- `instance_profiles` - 클라우드 인스턴스에 연결된 인스턴스 프로파일 목록
- `policies` - 사용자, 그룹, 역할 및 리소스에 권한을 할당하는 정책

예제

```
{
  "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"
      }
    ]
  }
}
```

# Security Hub의 적용 범위 조사 결과

Security Hub에 대한 적용 범위 조사 결과를 통해 어떤 AWS 보안 기능이 활성화되고 독립 실행형 계정 또는 조직의 멤버 계정에서 적용 범위에 격차가 있을 수 있는지 파악할 수 있습니다. 적용 범위 조사 결과는 현재 Amazon GuardDuty, Amazon Inspector, Amazon Macie 및 AWS Security Hub CSPM에 대해 활성화된 서비스 및 기능 보고를 지원합니다. 이러한 조사 결과는 Security Hub 대시보드의 보안 적용 범위 위젯에 표시되며 특정 보안 기능별로 더 세부적인 보기로 드릴다운할 수 있습니다.

제한 사항

- 멤버 계정의 경우 적용 범위 정보는 연결된 간에 집계 AWS 리전되지만 해당 멤버 계정에 대해서만 집계됩니다.

- Security Hub에 온보딩되지 않은 계정에는 적용 범위 정보가 표시되지 않습니다.

## AWS Security Hub CSPM에 대한 적용 범위 조사 결과

Security Hub CSPM 적용 범위 조사 결과는 계정에서 정규화된 태세 관리 보안 표준이 활성화되어 있는지 여부를 평가합니다. Security Hub CSPM 표준을 활성화하면 AWS Control Tower 및 리소스 태그 지정 표준을 제외하고 자격이 부여됩니다.

Security Hub CSPM을 활성화할 때 기본적으로 활성화된 표준을 감지하는 데 최대 24시간이 걸릴 수 있습니다.

## Amazon GuardDuty의 적용 범위 조사 결과

GuardDuty 적용 범위 조사 결과는 GuardDuty가 활성화되었는지 여부 및 AWS 계정에서 활성화된 GuardDuty 기능을 평가합니다.

- Amazon EC2용 GuardDuty 맬웨어 보호 - Amazon EC2 인스턴스에 잠재적 맬웨어가 있는지 스캔합니다.
- GuardDuty Amazon EKS 보호 - Amazon EKS 클러스터의 위협에 대한 Kubernetes 감사 로그를 모니터링합니다.
- GuardDuty Lambda 보호 - 잠재적 위협에 대한 Lambda 함수 호출을 분석합니다.
- GuardDuty Amazon S3 보호 - Amazon S3 버킷에 대한 잠재적 위협에 대한 데이터 이벤트를 분석합니다.
- GuardDuty Amazon RDS 보호 - Amazon RDS 데이터베이스에 대한 위협을 모니터링합니다.
- GuardDuty 런타임 모니터링 - Amazon EC2 인스턴스의 런타임 동작을 실시간으로 모니터링합니다.
- GuardDuty 기본 적용 범위 - GuardDuty가 활성화되면 자동으로 켜지는 기본 GuardDuty 기능입니다.

> **Note**
>
> GuardDuty 기본 적용 범위의 경우, 이 기능이 꺼져 있음을 나타내는 적용 범위 조사 결과는 해당 계정에서 GuardDuty가 활성화되지 않았음을 의미합니다.

GuardDuty 적용 범위 업데이트가 조직의 모든 멤버 계정에 반영되려면 최대 24시간이 걸릴 수 있습니다.

## Amazon Inspector의 적용 범위 조사 결과

Amazon Inspector 적용 범위 조사 결과는 Amazon Inspector가 활성화되었는지 여부 및 계정에서 활성화된 기능을 평가합니다.

- Inspector EC2 스캔 - Amazon EC2 인스턴스에 취약성이 있는지 스캔합니다.
- Inspector ECR 스캔 - Amazon ECR 컨테이너 이미지에 취약성이 있는지 스캔합니다.
- Inspector Lambda 표준 스캔 - Lambda 함수의 취약성을 스캔합니다.
- Inspector Lambda 코드 스캔 - Lambda 코드 함수에서 코드 취약성을 스캔합니다.

## Amazon Macie의 적용 범위 조사 결과

Macie 적용 범위 조사 결과는 AWS 계정에서 Macie가 활성화되었는지 여부를 평가합니다.

- Macie 민감한 데이터 자동 검색 적용 범위 - Amazon S3 데이터 자산에서 민감한 데이터를 지속적으로 평가합니다.

Macie 민감한 데이터 자동 검색 적용 범위 조사 결과에 대한 업데이트가 조직의 모든 멤버 계정에 반영되려면 최대 24시간이 걸릴 수 있습니다.

## 적용 범위 조사 결과 억제

기본적으로 보안 적용 범위 조사 결과는 계정 및 리전에 대해 활성화된 Amazon GuardDuty, Amazon Inspector, Amazon Macie 및 AWS Security Hub CSPM 기능을 평가합니다. 특정 보안 기능이 적용되지 않거나 허용되는 위험인 경우 억제 기능을 사용하여 다른 모든 결과와 유사한 적용 범위 조사 결과를 억제할 수 있습니다. 적용 범위 조사 결과가 표시되지 않으면 보안 적용 범위 위젯 내의 적용 범위 계산에 포함되지 않습니다. 위젯에는 억제된 적용 범위 조사 결과를 통해 보안 기능에 대한 적용 범위가 제외되었습니다라는 메시지가 표시됩니다. 메시지에는 억제된 결과 수가 포함됩니다.

Security Hub에서 적용 범위 조사 결과를 억제하려면

1. 보안 적용 범위 위젯을 볼 때 적용 범위 백분율 링크를 선택합니다.
2. 적용 범위 팝업에서 적용 범위 조사 결과 보기를 선택합니다. 상태가 새로 만들기인 각 결과는 관찰된 적용 범위 차이를 간략하게 설명합니다.
3. 억제하려는 각 결과 옆의 확인란을 선택합니다.
4. 페이지 상단에서 상태 업데이트를 선택한 다음 억제됨을 선택합니다.

5. 상태를 억제됨으로 설정 대화 상자에서 선택적으로 상태를 변경하는 이유를 자세히 설명하는 메모를 입력합니다. 그런 다음 상태 설정을 선택합니다.

# Security Hub의 AI 인벤토리

AWS Security Hub의 AI 인벤토리는 AWS 환경 전반의 인공 지능(AI) 및 기계 학습(ML) 리소스에 대한 통합 보기를 제공합니다. AI 인벤토리를 사용하여 승인되지 않은 AI 워크로드를 식별하고, AI가 실행 중인 위치와 검색 방법을 이해하고, 보안 검토가 더 필요한 리소스의 우선순위를 지정합니다. Security Hub는 AI 리소스를 두 가지 검색 유형으로 구성합니다.

- 관리형 -가 관리형 서비스로 AWS 제공하는 AI 리소스입니다. Security Hub는 AWS Config 구성 항목에서 이러한 리소스를 검색합니다. 관리형 리소스 유형에는 지원되는 Amazon Bedrock, Amazon Bedrock AgentCore 및 Amazon SageMaker의 하위 집합이 포함됩니다.
- 자체 호스팅 - 관리형 서비스로 제공되지 않는 AI 리소스입니다. 자체 컴퓨팅에서 실행되는 오픈 소스 모델, 에이전트 및 추론 서버를 예로 들 수 있습니다. Security Hub는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 및 Amazon Elastic Container Registry(Amazon ECR) 이미지에서 이러한 리소스를 감지합니다. 신호에는 Amazon Inspector 소프트웨어 재료표(SBOM) 조사 결과와 Amazon GuardDuty DNS 활동이 포함됩니다.

관리자 계정은 조직의 활성화된 모든 계정에서 AI 리소스를 볼 수 있습니다. 멤버 계정은 자신의 계정 내에서 AI 리소스만 볼 수 있습니다.

## 자체 호스팅 AI 검색을 위한 사전 조건

관리형 AI 리소스를 검색하면 Security Hub를 활성화하는 것 외에 추가 구성이 필요하지 않습니다. 자체 호스팅 AI 리소스를 검색하려면 기여 신호를 AWS 서비스 제공하는 도 활성화해야 합니다.

- Amazon Inspector - Amazon Inspector(Security Hub 필수 항목 포함)를 활성화하여 SBOMs 생성합니다. Security Hub는 이러한 SBOMs을 사용하여 자체 호스팅 모델, 추론 엔드포인트 및 에이전트를 감지합니다. Amazon EC2 인스턴스의 경우 향상된 스캔 모드, 에이전트 없는 스캔 또는 하이브리드 스캔을 사용하여 에이전트 기반 스캔을 활성화합니다. 고급 스캔 모드가 없는 에이전트 기반 스캔은 AI 리소스 감지에 필요한 심층 소프트웨어 인벤토리를 생성하지 않습니다. Amazon ECR 이미지의 경우 Amazon Inspector는 컨테이너 이미지 스캔을 통해 SBOMs 제공합니다.
- Amazon GuardDuty - Security Hub가 DNS 활동을 사용하여 Amazon EC2 인스턴스가 호출하는 외부 AI 엔드포인트를 감지할 수 있도록 GuardDuty를 활성화합니다.

# 지원되는 AI 리소스 유형

Security Hub는 정식 출시 시 다음과 같은 자체 호스팅 AI 리소스 유형을 지원합니다. Security Hub는 자체 호스팅 AI 리소스에 신뢰도 기반 탐지 시스템을 사용합니다. 각 감지는 SBOM 구성 요소와 같은 기본 신호에 고정됩니다. 그런 다음 Security Hub는 추가 신호를 상호 연관시켜 리소스가 인벤토리에 표시되기 전에 신뢰도를 설정합니다. Security Hub는 신뢰도 임계값을 충족하는 리소스만 표시하므로 거짓 긍정을 최소화하는 데 도움이 됩니다. 각 리소스는 `SelfHosted::AI::` 접두사`ResourceType`와 함께를 사용합니다.

- 모델(`SelfHosted::AI::Model`) - Hugging Face 및 Ollama 모델. Security Hub는 기본 모델 캐시 디렉터리(예: Hugging Face 및 Ollama 캐시)와 Amazon Inspector 스캔을 위해 구성한 사용자 지정 경로에서만 모델을 감지합니다.
- 추론 엔드포인트(`SelfHosted::AI::InferenceEndpoint`) - vLLM, Ollama, TorchServe, Triton, Text Generation Inference(TGI), SGLang, llama.cpp, LocalAI, BentoML, Xinference, Ray Serve 및 GPT4All과 같은 지원되는 모델 서비스 소프트웨어입니다.
- 에이전트(`SelfHosted::AI::Agent`) - OpenClaw 에이전트.
- 외부 엔드포인트(`SelfHosted::AI::ExternalEndpoint`) - Amazon EC2 인스턴스가 호출하는 외부 AI 서비스 도메인입니다. Security Hub는 OpenAI, Anthropic, Cohere, Mistral 및 기타 주요 AI 공급자와 같은 알려진 AI 서비스 도메인의 허용 목록을 유지 관리하고 인스턴스가 DNS 요청을 하는 시기를 감지합니다. 외부 엔드포인트는 Amazon EC2의 GuardDuty DNS 활동에서만 감지됩니다.

관리형 AI 리소스는 각각 `AI/ML` 리소스 범주가 있는 Amazon Bedrock, Amazon Bedrock AgentCore 및 Amazon SageMaker 구성 항목 유형의 지원되는 하위 집합입니다.

## 리소스 페이지에서 AI 리소스 찾기

리소스 페이지에는 환경의 모든 리소스가 나열됩니다. AI 리소스의 경우 다음 기능을 사용하여 AI 워크로드와 이를 실행하는 호스트를 식별할 수 있습니다.

- 관리형 AI/ML 리소스는 리소스 옆에 AI 아이콘을 표시합니다. 아이콘을 선택하여 설명을 봅니다.
- Amazon EC2 인스턴스와 같이 자체 호스팅 AI 리소스를 실행하는 호스트 리소스에는 자체 호스팅 AI 수 배지가 표시됩니다. 자체 호스팅 AI 리소스가 없는 호스트에는 배지가 표시되지 않습니다.
- 빠른 필터 토글을 사용하여 자체 호스팅 AI 리소스가 포함된 호스트만 표시합니다.
- 호스트로 드릴다운하려면 호스트를 선택하여 세부 정보 패널을 열고 AI 자산 탭을 선택한 다음 모두 보기를 선택하여 해당 호스트에서 감지된 자체 호스팅 AI 리소스를 확인합니다.

# AI 인벤토리 페이지 사용

AI 인벤토리 페이지는 조직의 AI 리소스에 중점을 둡니다. 이 페이지의 모든 리소스는 AI/ML 리소스 범주에 속합니다. 이 페이지에는 환경의 관리형 AWS AI 리소스와 자체 호스팅 AI 리소스가 표시됩니다. 다음 섹션에서는 페이지의 주요 구성 요소에 대해 설명합니다.

## 요약 표시줄

요약 표시줄에는 AI 자산의 총 수와 자체 호스팅 또는 관리형 검색 유형별 분류가 표시됩니다. 또한 모델 또는 에이전트와 같은 하위 범주별로 분류를 표시합니다. 통계 값을 선택하여 테이블에 지원 세부 정보를 표시합니다.

## 그룹화, 필터링 및 검색

AI 인벤토리 테이블은 기본적으로 리소스 유형별로 리소스를 그룹화합니다. 그룹화를 수정하거나 제거하여 모든 리소스를 평면적으로 볼 수 있습니다. 사용 가능한 그룹화 필드에는 정식 ID, 호스트 리소스 유형, 검색 유형, 계정 ID 및 리소스 유형이 포함됩니다.

정식 ID는 리소스가 실행되는 위치와 관계없이 리소스를 식별합니다. 예를 들어 동일한 Hugging Face 모델을 실행하는 두 Amazon EC2 인스턴스는 동일한 정식 ID를 공유하므로 조직 전체에서 특정 모델의 모든 배포를 찾을 수 있습니다.

> **Note**
>
> 정식 ID 및 호스트 리소스 유형 그룹화는 자체 호스팅 리소스에만 적용됩니다. 이러한 필드를 기준으로 그룹화하면 관리형 AI 리소스에는 이러한 속성이 없으므로 결과에 표시되지 않습니다. 검색 유형 또는 리소스 유형 그룹화를 사용하여 관리형 리소스와 자체 호스팅 리소스를 함께 확인합니다.

빠른 필터를 사용하면 리소스 하위 범주 또는 검색 유형별로 필터링할 수 있습니다. 속성 필터는 호스트 리소스 유형 및 자체 호스팅 리소스의 정식 ID를 포함한 추가 필드를 지원합니다.

## 리소스 세부 정보 및 기여 신호

리소스 행을 선택하여 세부 정보 패널을 엽니다. 관리형 리소스의 경우 패널에 리소스 구성이 JSON으로 표시됩니다. 자체 호스팅 리소스의 경우 패널에는 Security Hub가 리소스를 감지하는 데 사용한 기여 신호가 표시됩니다. 이러한 신호에는 SBOM 구성 요소 및 모델에 대한 지원 추론 소프트웨어 또는 외부 엔드포인트에 대한 DNS 도메인과 같은 탐지 소스 및 개별 신호 세부 정보가 포함됩니다.

### 호스트 리소스로 롤업

자체 호스팅 AI 리소스의 경우 세부 정보 패널에는 Security Hub가 리소스를 감지한 호스트 리소스가 표시됩니다. 동일한 호스트에서 자체 호스팅된 모든 AI 리소스를 보려면 호스트 리소스를 기준으로 테이블을 필터링합니다. 이 보기를 사용하면 개별 자체 호스팅 리소스에서 호스트로 드릴업하고 해당 호스트의 인접 AI 리소스를 검토할 수 있습니다.

## 고려 사항

AI 인벤토리는 정식 출시 시 다음과 같은 제한 사항이 있습니다.

- 이 릴리스에는 자체 호스팅 AI 리소스에 조사 결과가 없습니다. Security Hub는 관리형 AI 리소스에 대한 조사 결과 수만 표시합니다.
- 자체 호스팅 AI 감지는 Amazon EC2 인스턴스 및 Amazon ECR 이미지에서만 지원됩니다. AWS Lambda 함수 및 기타 컴퓨팅 유형은 지원되지 않습니다.
- Security Hub는이 릴리스의 상위 호스트에 Amazon ECR 이미지를 속성화하지 않으므로 호스트 AI 수에 포함되지 않습니다.
- Security Hub는 Amazon EC2의 GuardDuty DNS 활동에서만 외부 엔드포인트를 감지합니다. 이 릴리스에서 Security Hub는 AWS Fargate, Amazon SageMaker AWS Lambda, Amazon EKS 또는 기타 서비스 관리형 컴퓨팅의 호출을 속성으로 지정하지 않습니다.

## API를 사용하여 AI 인벤토리에 액세스

GetResourcesV2 및 GetResourcesStatisticsV2 작업을 사용하여 프로그래밍 방식으로 AI 인벤토리 데이터를 검색할 수 있습니다.

AI/ML 리소스의 경우 `GetResourcesV2` 응답에는 `ResourceSubCategory` 및 `DiscoveryType` 필드가 포함됩니다. `DiscoveryType` 필드는 리소스가 `Managed` 인지 또는 인지 여부를 나타냅니다`SelfHosted`. 자체 호스팅 AI 리소스 및 해당 호스트 리소스의 경우 응답에는 `AIDetails` 구조`ResourceInfo`도 포함됩니다.

자체 호스팅 AI 리소스는 `SelfHosted::AI::` 접두사`ResourceType`와 함께를 사용합니다. 지원되는 유형은 다음과 같습니다.

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

- SelfHosted::AI::ExternalEndpoint

AIDetails 구조는 HostResourceGuid 및 HostResourceType 필드를 사용하여 자체 호스팅 AI 리소스를 호스트에 연결합니다. CanonicalId 필드는 리소스가 배포된 위치와 관계없이 리소스를 식별하므로 여러 호스트에서 동일한 리소스를 집계할 수 있습니다. 정식 ID는 type/identifier 형식을 사용합니다.

- ML 모델의 경우: model/<purl> (예: model/pkg:huggingface/meta-llama/llama-3-8b)
- 추론 엔드포인트 및 에이전트의 경우: type/asset-identifier-name 형식
- 외부 엔드포인트의 경우: 정규화된 도메인(예: api.*.openai.com)

Amazon EC2 인스턴스와 같은 호스트 리소스에서 SelfHostedAI*ResourceCount 필드와 SelfHostedTotalAIResourceCount 필드에는 호스트에서 감지된 자체 호스팅 AI 리소스 수가 포함됩니다.

> **Note**
>
> GetResourcesV2를 사용하고 기준으로 필터링ResourceSubCategory하는 경우 ResourceCategory 필터도 포함해야 합니다. 비교를 로 EQUALS 설정하고 값을 로 설정합니다AI/ML. 이 요구 사항은 ResourceSubCategory에서 ResourceInfo.AIDetails.HostResourceType, 또는 ResourceInfo.AIDetails.CanonicalId를 기준으로 그룹화할 때도 적용됩니다GetResourcesStatisticsV2. 그렇지 않으면 작업이를 반환합니다ValidationException.
> 다음 예제에서는 유효한 필터 조합을 보여줍니다.

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

```
                    },
                    {
                        "FieldName": "ResourceSubCategory",
                        "Filter": {
                            "Comparison": "EQUALS",
                            "Value": "Model"
                        }
                    }
                ]
            }
        ]
    }
}
```

# Security Hub의 노출 조사 결과

Security Hub의 노출 결과는 AWS 환경의 잠재적 보안 위험을 식별하는 여러 보안 신호의 상관관계를 나타냅니다. 노출 결과는 보안 위험을 이해하고 우선순위를 정하는 데 도움이 됩니다. 취약성, 구성, 위협 및 리소스 관계의 조합을 자동으로 분석합니다. 노출 조사 결과에는 특성과 신호가 포함됩니다. 신호에는 여러 유형의 노출 특성이 포함될 수 있습니다. Security Hub는 Security Hub CSPM, Amazon Inspector, GuardDuty, Macie 또는 기타 AWS 서비스의 신호가 노출이 있음을 나타낼 때 노출 결과를 생성합니다. 리소스는 최대 하나의 노출 조사 결과에서 기본 리소스일 수 있습니다. 리소스에 노출 특성이 없거나 특성이 부족한 경우 Security Hub는 해당 리소스에 대한 노출 결과를 생성하지 않습니다.

## 노출 조사 결과의 작동 방식

Security Hub는 다음을 통해 노출 조사 결과를 생성합니다.

여러 AWS 보안 서비스의 신호 분석

Security Hub는 여러 보안 서비스에서 AWS 보안 신호를 지속적으로 수집하고 분석합니다. 위협 탐지를 위해 GuardDuty, 취약성 평가를 위해 Amazon Inspector, 구성 확인을 위해 Security Hub CSPM, 민감한 데이터 노출을 위해 Macie의 결과를 수집합니다. 이러한 신호는 잠재적 보안 위험을 식별하기 위해 고급 상관관계 엔진을 통해 처리됩니다.

리소스 구성 및 관계 평가

시스템은 보안 모범 사례를 기준으로 리소스 구성에 대한 자세한 평가를 수행합니다. 서비스별 설정, 규정 준수 요구 사항 및 보안 제어를 검사합니다. 이 분석은 다른 요인과 결합할 때 보안 취약성으로 이어질 수 있는 잘못된 구성을 식별하는 데 도움이 됩니다.

네트워크 연결성 평가

노출 조사 결과의 중요한 구성 요소는 네트워크 연결성 평가입니다. 시스템은 인터넷 노출 및 내부 네트워크 액세스 경로를 모두 평가합니다. 보안 그룹 구성 및 네트워크 ACL 설정을 분석하여 잠재적 공격 벡터를 결정합니다. 이 분석은 무단 액세스에 실수로 노출될 수 있는 리소스를 식별하는 데 도움이 됩니다.

관련 보안 문제 상호 연결

상관관계 엔진은 AWS 리소스 간의 관계를 매핑하여 리소스가 상호 작용하는 방식을 분석하고 잠재적 보안 영향을 식별합니다. IAM 권한, 역할 및 리소스 액세스 패턴을 검사하여 광범위한 보안 컨텍스트를 이해합니다. 이 프로세스는 무해해 보이는 개별 구성의 조합으로 인해 존재할 수 있는 보안 위험을 식별하는 데 도움이 됩니다.

## 노출 조사 결과의 구성 요소

각 노출 결과에는 다음이 포함됩니다.

잠재적 보안 위험의 제목 및 설명

각 노출 결과에는 보안 위험의 특성을 즉시 전달하는 명확하고 설명적인 제목이 포함되어 있습니다. 설명은 잠재적 보안 영향, 영향을 받는 리소스 및 노출의 광범위한 컨텍스트에 대한 자세한 정보를 제공합니다. 이 정보는 보안 팀이 위험을 신속하게 이해하고 평가하는 데 도움이 됩니다.

심각도 분류(심각, 높음, 중간, 낮음)

- 심각한 심각도는 악용 가능성이 높고 상당한 잠재적 영향으로 인해 즉각적인 주의가 필요함을 나타냅니다. 이러한 결과는 일반적으로 쉽게 발견하고 악용할 수 있는 취약성을 나타냅니다.
- 심각도가 높으면 우선 순위 주의가 필요하며, 악용 가능성이 중간에서 높고 상당한 잠재적 영향이 있음을 시사합니다. 이러한 결과는 비교적 악용하기 쉽지만 특정 조건이 필요할 수 있습니다.
- 중간 심각도는 악용 가능성이 낮고 잠재적 영향이 중간 정도이며 예약된 주의가 필요함을 나타냅니다. 이러한 조사 결과에는 일반적으로 더 복잡한 악용 방법이 필요합니다.
- 심각도가 낮으면 악용 가능성이 제한되고 경미한 영향과 함께 일상적인 주의가 필요함을 시사합니다. 이러한 결과는 일반적으로 악용하기 어렵고 위험을 최소화합니다.

노출로 이어진 특성 기여

기여 특성은 노출 조사 결과를 초래한 주요 요인을 나타냅니다. 여기에는 직접적인 보안 취약성, 구성 문제, 네트워크 노출 조건 및 리소스 권한 설정이 포함됩니다. 각 특성은 전반적인 보안 위험에 어떻게 기여하는지에 대한 구체적인 세부 정보를 제공합니다.

잠재적 공격 경로 및 블래스트 반경 시각화

잠재적 공격 경로 및 폭발 반경 시각화는 잠재적 공격자가 식별된 노출을 악용할 수 있는 방법을 보여주는 대화형 다이어그램을 제공합니다. 리소스 관계, 네트워크 경로 및 권한 에스컬레이션 경로를 공격자가 노출을 악용할 경우 잠재적으로 액세스할 수 있는 다운스트림 리소스에 매핑합니다.

자세한 문제 해결 지침

각 노출 결과에는 식별된 위험을 해결하기 위한 구체적이고 실행 가능한 단계가 포함된 자세한 해결 지침이 포함되어 있습니다. 이 지침에는 모범 사례 권장 사항, 구성 수정 단계 및 우선 순위가 지정된 작업 항목이 포함되어 있습니다. 이 지침은 특정 노출 시나리오에 맞게 조정되며 관련된 AWS 서비스를 고려합니다.

리소스 구성 세부 정보

조사 결과가 생성된 시점의 리소스 구성과 Security Hub 리소스 인벤토리 대시보드에서 리소스의 현재 구성입니다.

추가 보안 컨텍스트를 제공하는 컨텍스트 특성

컨텍스트 특성은 Security Hub에서 식별했지만 노출 조사 결과를 생성하는 데 사용되지 않은 추가 보안 마커입니다.

IAM Access Analyzer의 미사용 액세스 정보는 노출 조사 결과에 컨텍스트 특성으로 나타날 수 있습니다. 리소스에 연결된 IAM 역할에 미사용 권한이 있는 경우 Security Hub는이 정보를 노출 세부 정보 보기에 컨텍스트 특성으로 포함합니다. 예를 들어 Amazon EC2 인스턴스에 소프트웨어 취약성이 있고 연결된 IAM 역할에 5개 서비스에서 47개의 미사용 권한이 있는 경우 노출 결과에 미사용 권한이 보조 컨텍스트로 표시됩니다. 이렇게 하면 잠재적 폭발 반경을 이해하는 데 도움이 됩니다. 과도하게 권한이 부여된 IAM 역할이 있는 취약한 리소스는 최소 권한이 있는 리소스보다 위험이 높습니다. 손상된 리소스는 이러한 미사용 권한을 사용하여 액세스를 에스컬레이션할 수 있기 때문입니다.

다음 리소스 유형은 노출 결과에 미사용 액세스 컨텍스트 특성을 표시할 수 있습니다.

- Amazon Elastic Compute Cloud 인스턴스
- AWS Lambda 함수
- Amazon Elastic Container Service 서비스
- Amazon Elastic Kubernetes Service 클러스터
- IAM 사용자(직접)

# 심각도 분류

노출 결과는 다음을 기준으로 분류됩니다.

- 검색 용이성
- 악용 용이성
- 악용 가능성
- 대중 인식
- 잠재적 영향

자세한 내용은 노출 결과 심각도 분류를 참조하세요.

## 노출 조사 결과의 이점

- 자동 상관 관계를 통한 수동 분석 감소: 노출 조사 결과는 자동 상관 관계 및 지능형 위험 우선 순위를 통해 보안 분석에 필요한 시간과 노력을 크게 줄입니다. Security Hub는 AWS 환경을 지속적으로 모니터링하여 수동 검토를 통해 놓칠 수 있는 보안 위험을 자동으로 식별하고 상호 연관시킵니다.
- 보안 위험의 우선순위 보기: Security Hub는 정교한 위험 평가 알고리즘을 사용하여 심각도, 영향, 리소스 중요도 및 악용 가능성에 따라 노출의 우선순위를 지정합니다. 이를 통해 보안 팀은 가장 중요한 위험에 먼저 집중하여 보안 운영의 효율성을 개선할 수 있습니다.

## 노출 조사 결과의 출처

노출 조사 결과에는 다음 데이터가 포함됩니다.

- Amazon GuardDuty 통합은 노출 조사 결과 내에서 지속적인 위협 탐지 기능을 제공합니다. 악의적인 활동, 잠재적 계정 손상 및 동작 이상을 모니터링합니다. 시스템은 이러한 위협 조사 결과를 더 광범위한 노출 분석에 통합하여 위협이 다른 보안 문제와 결합하여 심각한 위험을 생성하는 시기를 식별하는 데 도움이 됩니다.
- Amazon Inspector는 노출 결과에 중요한 취약성 평가 데이터를 제공합니다. 네트워크 연결성, 소프트웨어 취약성 및 보안 모범 사례 위반에 대한 자세한 정보를 제공합니다. 이 통합은 식별된 공격 경로를 통해 취약성이 어떻게 악용될 수 있는지 이해하는 데 도움이 됩니다.
- AWS Security Hub CSPM은 노출 분석에서 구성 규정 준수 및 보안 표준을 고려하도록 보장합니다. 설정된 보안 제어 및 모범 사례를 기준으로 리소스를 평가하여 구성 기반 위험을 이해하기 위한 기반을 제공합니다.

- Amazon Macie는 민감한 데이터 검색 및 분류 기능으로 노출 조사 결과를 개선합니다. AWS 환경 내에서 민감한 데이터가 존재하는 위치를 식별하고 잠재적 프라이버시 위험을 평가하여 식별된 노출의 잠재적 영향을 이해하는 데 도움이 됩니다.

## 모범 사례

- 노출 조사 결과를 정기적으로 검토: 효과적인 노출 관리를 위해서는 구조화된 검토 프로세스가 필요합니다. 조직은 중요한 노출에 대한 일일 검토, 전체 노출 상태에 대한 주간 평가, 월별 추세 분석 및 분기별 보안 태세 평가를 구현해야 합니다. 이 계층화된 접근 방식은 즉각적인 위험과 장기 보안 추세 모두에 적절한 주의를 기울입니다.
- 중요하고 심각도가 높은 노출의 우선 순위 지정: 성공적인 노출 관리는 효과적인 위험 우선 순위 지정에 따라 달라집니다. 조직은 먼저 리소스 중요도와 비즈니스 영향을 고려하면서 중요한 노출에 집중해야 합니다. 이러한 위험 기반 접근 방식은 보안 노력이 비즈니스 우선순위에 부합하도록 하고 위험 감소를 극대화하는 데 도움이 됩니다.
- 권장 문제 해결 단계 구현: 노출 문제 해결은 체계적인 접근 방식을 따라야 합니다. 조직은 권장 수정 단계를 신중하게 구현하고, 변경 사항에 대한 자세한 문서를 유지하고, 수정 사항에 대한 철저한 테스트를 수행하고, 구현된 수정의 효과를 검증해야 합니다. 이 체계적인 접근 방식은 의도하지 않은 결과를 방지하면서 성공적인 위험 완화를 보장하는 데 도움이 됩니다.
- 자동 응답 규칙 구성: 노출 결과의 가치를 극대화하려면 효과적인 자동화가 필요합니다. 조직은 자동 응답 규칙을 구현하고, 적절한 알림을 구성하고, 효율적인 워크플로를 설정하고, 포괄적인 감사 추적을 유지해야 합니다. 이 자동화를 통해 식별된 노출에 일관되고 시기 적절한 대응을 보장하는 동시에 수동 작업을 줄일 수 있습니다.

## Security Hub의 노출 조사 결과에 대해 지원되는 리소스 유형

AWS Security Hub는 다음 유형의 AWS 리소스에 대한 노출 조사 결과를 생성합니다.

- `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`

Azure 커넥터가 있는 경우 Security Hub는 다음 유형의 Azure 리소스에 대한 노출 조사 결과도 생성합니다.

- `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 Hub는 기본 리소스당 하나의 노출 조사 결과를 생성합니다. 리소스에 노출 특성이 없거나 특성이 부족한 경우 Security Hub는 해당 리소스에 대한 노출 결과를 생성하지 않습니다.

## Security Hub에서 지원되는 특성 유형

AWS Security Hub는 AWS Security Hub CSPM 제어 조사 결과 및 Amazon Inspector AWS 서비스와 같이 지원되는 다른에서 생성된 조사 결과에 리소스에 대한 노출 특성이 포함된 경우 노출 조사 결과를 생성합니다. 다음 표에서는 지원되는 특성 유형에 대한 정보를 제공합니다.

| 특성 유형 | 설명 | 소스 | 영향을 받는 리소스 |
|---|---|---|---|
| 가정성 | 판매 권한이 있는 리소스를 나타냅니다 AWS Identity and Access Management . | 의 리소스 구성 AWS Config | AWS 연결된 AWS Identity and Access Management 역할이 있는 리소스 |
| 영향 | 리소스를 생성하고 수정하는 기능을 포함하여 연결된 AWS Identity and | 연결된 AWS Identity and | AWS 관련 AWS Identity |

| 특성 유형 | 설명 | 소스 | 영향을 받는 리소스 |
| --- | --- | --- | --- |
| | Access Management 보안 주체의 유효 권한을 기반으로 리소스가 손상된 경우 잠재적 블래스트 반경을 나타냅니다. | Access Management 보안 주체의 효과적인 권한 분석 | and Access Management 자격 증명이 있는 리소스 |
| 잘못된 구성 | 잘못 구성된 리소스를 나타냅니다. | AWS Security Hub CSPM 제어 조사 결과, Amazon GuardDuty 위협 조사 결과 및의 리소스 확인에 대한 정보 AWS Config. | 모든 리소스 유형 |
| 연결성 | 리소스에 대한 열린 네트워크 경로를 나타냅니다. | AWS Security Hub CSPM 제어 조사 결과, Amazon GuardDuty 위협 조사 결과 및 Amazon Inspector 네트워크 연결성 조사 결과. | Amazon EC2 인스턴스, Amazon EKS 클러스터, Lambda 함수 및 Amazon S3 버킷 |
| 민감한 데이터 | 리소스에 민감한 데이터가 포함되어 있음을 나타냅니다. | Macie의 민감한 데이터 조사 결과 | Amazon S3 버킷 |

| 특성 유형 | 설명 | 소스 | 영향을 받는 리소스 |
| --- | --- | --- | --- |
| 취약성 | 리소스에 위협 소스에 의해 악용될 수 있는 약점이 있음을 나타냅니다. | Amazon Inspector는 취약성 조사 결과와 Amazon GuardDuty Amazon EC2 맬웨어 조사 결과를 패키징합니다. | Amazon EC2 인스턴스, Amazon ECS 서비스, Amazon EKS 클러스터, Lambda 함수 |

각 특성은 리소스에 영향을 미치는 노출에 대한 세부 정보를 제공하는 여러 제목과 연결될 수 있습니다. 예를 들어 EC2 노출 조사 결과의 세부 정보에서 취약성 특성에 대한 공격 가능 제목이 표시될 수 있습니다.

### 영향 및 유효 권한

영향 특성은 노출 결과의 기본 리소스가 손상된 경우 공격자가 도달하고 손상시킬 수 있는 다운스트림 리소스인 노출의 잠재적 폭발 반경을 설명합니다. 영향을 확인하기 위해 Security Hub는 리소스와 연결된 AWS Identity and Access Management (IAM) 보안 주체의 유효 권한을 분석합니다.

유효 권한은 Security Hub가 액세스할 수 있는 리소스의 리소스 기반 정책과 함께 자격 증명 기반 정책을 평가한 후 보안 주체가 실제로 갖는 권한입니다. 유효 권한은 보안 주체에게 부여된 것과 대상 리소스가 허용하는 것을 모두 고려하므로 보안 주체가 수행할 수 있는 작업을 자격 증명 기반 정책만 수행하는 것보다 더 정확하게 반영합니다.

Security Hub는 유효 권한을 사용하여 기본 리소스에서 환경의 다른 리소스로 권한 에스컬레이션 경로를 추적합니다. 각 경로는 공격자가 한 리소스에서 다음 리소스로 이동할 수 있도록 허용하는 권한에 의해 연결된 리소스 체인입니다. Security Hub는 기존 리소스에 대한 구체적인 경로를 식별하면 해당 경로를 영향 특성의 일부로 표시합니다. 또한 다른 리소스를 생성하거나 수정할 수 AWS 서비스 있는 호출 기능과 같이 이러한 경로 이상의 권한도 영향을 고려합니다. 잠재적 공격 경로 그래프에서 이러한 경로를 검토하고 불필요한 권한을 제거하여 블래스트 반경을 줄일 수 있습니다. 자세한 내용은 Security Hub에서 잠재적 공격 경로 그래프를 사용하여 노출 보기 단원을 참조하십시오.

# 노출 조사 결과 생성

Security Hub는 거의 실시간으로 노출 조사 결과를 생성합니다. 새로운 보안 조사 결과가 수집되고 기존 조사 결과가 업데이트되면 Security Hub는 거의 실시간으로 노출 조사 결과를 생성하거나 업데이트합니다. Security Hub는 리소스 ID당 하나의 노출 조사 결과를 생성합니다.

Security Hub는 노출 조사 결과에서 지원되지 않는 리소스 유형에 대한 노출 조사 결과를 게시하지 않습니다. 리소스에 특성의 개수 및 조합이 많이 있는 경우 Security Hub는 하나의 노출 조사 결과를 생성합니다. 특성의 개수 및 조합에 따라 노출 조사 결과의 심각도 수준도 결정됩니다.

## 샘플 노출 조사 결과

AWS Security Hub는 Open Cybersecurity Schema Framework(OCSF)의 노출 조사 결과를 정규화합니다.

샘플 노출 조사 결과

다음 샘플 노출 조사 결과에서 `related_events` 파라미터에는 기여 조사 결과와 같은 노출 조사 결과에 고유한 세부 정보가 포함되어 있습니다. 기여 조사 결과는 노출 조사 결과와 연결된 특성 및 신호입니다. 단일 기여 결과에 하나 이상의 특성이 포함될 수 있습니다. `observables` 파라미터는 기여 조사 결과와 연결된 리소스를 식별합니다. 이는 노출 조사 결과와 연결된 리소스를 식별하는 `resources` 파라미터와 다를 수 있습니다.

```
{
    "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"
    }
}
```


# 노출 조사 결과의 심각도 수준 결정

AWS Security Hub는 각 노출 조사 결과에 CRITICAL, HIGHMEDIUM, 또는의 기본 심각도를 할당합니다LOW. 심각도가 인 노출 결과는 게시INFORMATIONAL되지 않습니다. Security Hub는 위험 매트릭스에 대한 가능성과 영향이라는 두 가지 차원을 결합하여 노출 결과의 심각도를 결정합니다. 가능성은 노출이 얼마나 쉽게 악용될 수 있는지를 반영하고, 영향은 악용될 경우 피해의 정도를 반영합니다.

리소스에 대한 영향을 확인할 수 없는 경우 심각도는 전적으로 가능성에 따라 결정됩니다.

## 위험 매트릭스

다음 표는 노출 결과의 최종 심각도를 생성하기 위해 가능성과 영향을 결합하는 방법을 보여줍니다. 가능성으로 인해 기준 심각도가 설정되고 영향이 조정됩니다. 영향이 높으면 심각도가 한 수준씩 증가하고(로 제한됨CRITICAL), 영향이 중간이면 심각도가 변경되지 않고, 영향이 낮으면 심각도가 한 수준씩 감소합니다(로 중단됨INFORMATIONAL). 영향은 가능성의 심각도만 조정합니다. 영향만으로는 노출 조사 결과가 생성되지 않습니다.

심각도 위험 매트릭스

| 가능성 ™ / 영향 → | 낮음 | 중간 | 높음 |
|---|---|---|---|
| 매우 높음 | 높음 | 심각 | 심각 |
| 높음 | 중간 | 높음 | 심각 |
| 보통 | 낮음 | 중간 | 높음 |
| 낮음 | 정보 | 낮음 | 중간 |

> **Note**
>
> 가능성이 낮고 영향이 적으면 심각도가 입니다`INFORMATIONAL`. Security Hub는이 심각도의 노출 조사 결과를 게시하지 않으므로 노출 페이지 또는 GetFindingsV2 결과에 표시되지 않습니다.

## 가능성

가능성은 가정성, 잘못된 구성, 연결성, 민감한 데이터 및 취약성과 같이 리소스에 존재하는 기여 특성을 기반으로 노출을 얼마나 쉽게 악용할 수 있는지 측정합니다. Security Hub는 다음과 같은 몇 가지 특성을 사용하여 가능성을 평가합니다.

- 인식 - 노출이 이론적이지 않지만 공개적으로 사용 가능하거나 자동화된 악용이 있는 정도입니다.
- 검색 용이성 - 포트 스캔 또는 인터넷 검색과 같은 자동화된 도구를 사용하여 위험 리소스를 검색할 수 있는지 여부입니다.
- 악용 용이성 - 위협 행위자가 노출을 악용할 수 있는 용이성입니다. 예를 들어 개방된 네트워크 경로 또는 잘못 구성된 메타데이터가 있는 경우 위협 행위자는 노출을 더 쉽게 악용할 수 있습니다.
- 악용 가능성 - 향후 30일 이내에 노출이 악용될 가능성입니다. 이 요소는 EPSS(Exploit Prediction Scoring System)에 해당합니다.

## 영향

영향은 노출이 악용될 경우 환경에 미치는 유해 정도를 측정합니다. 예를 들어 노출은 책임 손실, 가용성 손실, 데이터 노출로 인한 신뢰성 손실 또는 데이터 손상으로 인한 무결성 손실을 초래할 수 있습니다.

영향을 평가하기 위해 Security Hub는 리소스와 연결된 보안 주체의 AWS Identity and Access Management 유효 권한을 분석하여 공격자가 호출할 수 있는 작업을 AWS 서비스 결정합니다. 또한 공격자가 권한 에스컬레이션을 통해 도달하고 침해할 수 있는 기존 리소스를 식별합니다. 자세한 내용은 영향 및 유효 권한 단원을 참조하십시오.

## 노출 조사 결과 검토

Security Hub 콘솔 및 GetFindingsV2 API를 사용하여 모든 노출 조사 결과를 검토할 수 있습니다. Security Hub 콘솔의 노출 페이지에는 모든 활성 노출 조사 결과가 표시됩니다. 노출 조사 결과는 심각도 기준으로 내림차순으로 나열됩니다. 필터 추가 검색 창을 사용하여 필터를 추가/제거하여 노출 조사 결과를 필터링할 수 있습니다. 그룹화 기준 드롭다운을 사용하여 노출 조사 결과를 그룹화할 수 있습니다. 빠른 필터 메뉴를 사용하여 노출 조사 결과를 필터링할 수도 있습니다.

### 노출 조사 결과에 대한 세부 정보

노출 조사 결과에 대한 다양한 세부 정보를 볼 수 있습니다. 이러한 세부 정보는 Security Hub 콘솔에서 탭으로 구분됩니다. 개요 탭은 노출 조사 결과에 대한 주요 세부 정보를 제공합니다. 특성 탭에는 노출 조사 결과와 연결된 특성 및 신호가 나열됩니다. 리소스 탭은 노출 조사 결과와 연결된 리소스 및 리소스 태그에 대한 세부 정보를 제공합니다. 다음 목록에서는 노출 조사 결과 세부 정보에 대한 설명을 제공합니다.

- 조사 결과 제목 - 노출 조사 결과의 제목입니다.
- 심각도 수준 - 노출 조사 결과의 심각도 수준입니다. Security Hub는 리소스에 대한 특성의 개수 및 조합을 사용하여 노출 조사 결과의 심각도 수준을 결정합니다. 심각도 수준은 `CRITICAL`, `HIGH`, `MEDIUM` 또는 `LOW`일 수 있습니다. Security Hub는 심각도가 인 노출 조사 결과를 게시하지 않습니다`INFORMATIONAL`. Security Hub 콘솔 또는 BatchUpdateFindingsV2 API 작업을 통해 `Severity`를 업데이트할 수 있습니다.
- 설명 - 노출 조사 결과에 대한 설명입니다.
- 유형 - 노출 조사 결과 유형의 이름입니다. 예를 들어, 이름은 `Exposure/Potential Impact/Resource Hijacking`과 비슷할 수 있습니다.
- 계정 - 노출 조사 결과가 생성된 AWS 계정 의 ID입니다.
- 경과 시간 - 노출 조사 결과가 활성화된 기간을 나타냅니다.
- 생성된 시간 - 노출 조사 결과가 생성된 시점을 나타내는 타임스탬프입니다.
- 수정된 시간 - 노출 조사 결과가 마지막으로 업데이트된 시점을 나타내는 타임스탬프입니다.
- 리전 - 노출 조사 결과가 생성된 AWS 리전 입니다.

- 제품 이름 - 노출 조사 결과를 생성한 제품의 이름입니다. 항상 Security Hub Exposure Detection입니다.
- 회사 이름 - 노출 조사 결과를 생성한 회사의 이름입니다. 항상 AWS입니다.
- 활동 이름 - 조사 결과에 대해 마지막으로 수행한 활동의 이름입니다.
- 상태 -이 노출 조사 결과의 상태입니다.
- 조사 결과 ID - 노출 조사 결과와 연결된 고유 식별자입니다.
- 잠재적 공격 경로(콘솔만 해당) - 잠재적 공격자가 노출 조사 결과와 연결된 리소스에 액세스하고 제어하는 방법을 보여주는 대화형 시각화입니다. 자세한 내용은 Security Hub에서 잠재적 공격 경로 그래프를 사용하여 노출 보기 단원을 참조하십시오.
- 특성 - 노출 조사 결과와 연결된 특성 유형 및 특성 제목을 식별합니다. Security Hub 콘솔에서 특성 유형 또는 신호별로 특성을 볼 수 있습니다. 이를 통해 관련 노출의 컨텍스트에서 기여 조사 결과를 분석할 수 있습니다.
- 문제 해결 - 노출에서 식별된 특성과 관련된 문제 해결 설명서에 대한 링크입니다.
- 리소스 - 노출 조사 결과와 연결된 리소스를 식별합니다.

## 노출 조사 결과에 대한 세부 정보 검토

이 주제에서는 AWS Security Hub 콘솔 및 API를 사용하여 노출 조사 결과에 대한 세부 정보를 검토하는 방법을 설명합니다.

### Security Hub 콘솔에서 노출 조사 결과에 대한 세부 정보 검토

Security Hub 콘솔에서 노출 조사 결과에 대한 세부 정보를 보려면

1. https://console.aws.amazon.com/securityhub/v2/home에서 자격 증명을 사용하여 로그인하고 Security Hub 콘솔을 엽니다.
2. 탐색 창에서 노출을 선택합니다.
3. 세부 정보를 보려는 노출 조사 결과를 선택합니다.

### API를 사용하여 노출 조사 결과에 대한 세부 정보 검토

GetFindingsV2 API 또는 AWS CLI를 사용하여 노출 조사 결과를 검토할 수 있습니다. `metadata.product.feature.uid` 필드에서 `security-hub/Exposure` 값을 사용하여 모든 노출 조사 결과를 필터링할 수 있습니다. 자세한 내용은 GetFindingsV2 단원을 참조하십시오.

명령 예제

다음은 계정에서 가장 최근에 생성된 노출 조사 결과 10개를 검색하는 AWS CLI 예입니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

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

## Security Hub에서 잠재적 공격 경로 그래프를 사용하여 노출 보기

잠재적 공격 경로 그래프는 잠재적 공격자가 노출 조사 결과와 연결된 리소스에 액세스하고 제어하는 방법을 보여주는 대화형 시각화입니다. 이 그래프는 Security Hub 콘솔의 노출 페이지에서만 액세스할 수 있습니다. 노출 조사 결과에 대한 세부 정보를 볼 때 개요 탭에는 잠재적 공격 경로 및 블래스트 반경이라는 섹션이 포함됩니다.

공격 경로 그래프에는 노출이 생성된 기본 리소스, 네트워크 경로(해당하는 경우), 공격자가 권한을 에스컬레이션하여 도달할 수 있는 다운스트림 리소스가 표시됩니다. Security Hub가 기본 리소스에서 환경의 다른 리소스로의 구체적인 권한 에스컬레이션 경로를 식별하면 그래프의 블래스트 반경 부분으로 표시됩니다. 각 노드는 리소스를 나타내며 노드 간 연결에는 공격자가 한 리소스에서 다음 리소스로 이동할 수 있는 권한이 표시됩니다.

개요 탭의 이 섹션에서는 잠재적 공격 경로 그래프에서 AWS 리소스를 선택하고 드래그할 수 있습니다. 확대 및 축소 아이콘을 사용하여 공격 경로 그래프의 특정 영역에 초점을 맞출 수 있습니다. 전체 화면 아이콘을 통해 전체 화면 모드에서 공격 경로 그래프를 확장할 수 있습니다. 범례는 기본 리소스, 관련 리소스, 폭발 반경 리소스 및 기여 특성 수를 색상별로 코딩하고 공격 경로 그래프에 특성 범주 및 특성 수를 표시합니다. 리소스를 선택하고 리소스 세부 정보 보기를 선택하여 리소스에 대한 세부 정보를 볼 수 있습니다. 리소스와 연결된 ID 및 AWS 계정 번호를 복사할 수도 있습니다. 연결성 특성이 있는 노출 조사 결과는 공격 경로 그래프에 퍼블릭 인터넷 및 축소된 네트워크 경로가 표시됩니다. 축소된 네트워크 경로 노드를 선택하여 이 세부 정보를 볼 수 있습니다.

다운스트림 리소스와 해당 리소스를 연결하는 권한 에스컬레이션 경로를 보려면 영향 평가 탭을 선택합니다. 각 경로에는 공격자가 통과할 수 있는 리소스 체인과 각 단계의 특정 권한이 표시됩니다. 영향 특성 및 유효 권한에 대한 자세한 내용은 섹션을 참조하세요영향 및 유효 권한.

## 노출 조사 결과 문제 해결

이 섹션의 주제에서는 다양한 노출 조사 결과에 대한 수정 단계를 설명합니다 AWS 서비스.

OCSF 형식의 `Remediation` 필드에는 2개의 필드 `remediation` 및 `references`가 있습니다.

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

> **Note**
>
> 다음 섹션에 제공된 문제 해결 지침에 따라 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

## DynamoDB 테이블에 대한 노출 문제 해결

AWS Security Hub는 DynamoDB 테이블에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 DynamoDB 테이블 및 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침은 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- DynamoDB의 잘못된 구성 특성

- DynamoDB 테이블에 특정 시점 복구가 비활성화됨
- DynamoDB 테이블을 백업 계획으로 보호되지 않음
- DynamoDB 테이블에 삭제 방지가 비활성화됨

### DynamoDB의 잘못된 구성 특성

다음은 DynamoDB 테이블의 잘못된 구성 특성 및 문제 해결 단계를 설명합니다.

#### DynamoDB 테이블에 특정 시점 복구가 비활성화됨

문제 해결: DynamoDB point-in-time 복구 활성화

DynamoDB 특정 시점 복구는 DynamoDB 테이블 데이터에 대한 지속적 자동 백업을 제공합니다. DynamoDB 테이블을 특정 시점으로 복원하는 방법에 대한 자세한 내용은 Amazon DynamoDB 개발자 안내서의 특정 시점으로 DynamoDB 테이블 복원을 참조하세요. DynamoDB

#### DynamoDB 테이블을 백업 계획으로 보호되지 않음

AWS Backup은 DynamoDB를 포함한 여러 서비스에서 백업을 구성, 관리 및 자동화하는 중앙 집중식 AWS 서비스를 제공합니다. 백업 계획이 없으면 테이블에 보존 기간을 사용자 지정 가능한 예약된 자동 백업이 없으므로 상당한 보안 위험이 발생합니다. 공격자는 테이블 데이터를 악의적으로 손상시키거나 삭제할 수 있습니다. 적절한 백업이 없으면 특정 시점 복구 기간(활성화된 경우)을 초과하는 복구 옵션이 없어 영구적인 데이터 손실이 발생할 수 있습니다. 데이터 보호 모범 사례에 따라 DynamoDB 테이블을 백업 계획으로 다룹니다.

문제 해결: 백업 계획 생성

백업 계획을 생성하기 전에 데이터에 대한 적절한 백업 빈도 및 보존 기간을 결정합니다. 백업 계획을 생성하는 방법에 대한 자세한 내용은 AWS 백업 개발자 안내서의 백업 계획에 리소스 할당을 참조하세요.

#### DynamoDB 테이블에 삭제 방지가 비활성화됨

삭제 방지는 DynamoDB 테이블이 실수로 삭제되는 것을 방지합니다. 삭제 방지가 비활성화되면 DynamoDB 테이블은 콘솔 작업, API 호출, CLI 명령 또는 자동 프로세스를 통한 의도하지 않은 삭제에 취약합니다. 이로 인해 AWS 환경에 액세스할 수 있는 권한이 없는 엔터티가 의도적으로 테이블을 삭제하여 서비스 중단과 영구적인 데이터 손실을 초래할 수 있으므로 AWS 환경이 데이터 손실에 노출될 수 있습니다. 데이터 보호 모범 사례에 따라 DynamoDB 테이블에 대한 데이터 보호를 활성화합니다.

문제 해결: 삭제 방지 활성화

여러 테이블을 관리하는 경우를 사용하여 테이블 속성을 대량으로 업데이트 CloudFormation 하는 것이 좋습니다. `DeletionProtectionEnabled` 속성을 포함하고 스택을 업데이트하도록 CloudFormation 템플릿을 수정할 수 있습니다. 문제 해결을 완료한 후 테이블 설정 탭의 추가 정보 드롭다운에서 삭제 방지가 활성화되어 있는지 확인합니다.

## EC2 인스턴스에 대한 노출 문제 해결

AWS Security Hub는 Amazon Elastic Compute Cloud(EC2) 인스턴스에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 EC2 인스턴스 및 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침은 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- EC2 인스턴스의 잘못된 구성 특성
  - EC2 인스턴스는 버전 1을 사용하여 IMDS에 대한 액세스를 허용합니다.
  - Amazon EC2 인스턴스에는 SSH 또는 RDP 액세스를 허용하는 보안 그룹 또는 네트워크 ACL이 있습니다
  - Amazon EC2 인스턴스에 개방형 보안 그룹이 있음
- EC2 인스턴스의 연결성 특성
  - EC2 인스턴스는 인터넷을 통해 연결할 수 있습니다
- EC2 인스턴스의 취약성 특성

  - EC2 인스턴스에 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있음
  - Amazon EC2 인스턴스에 소프트웨어 취약성이 있음
  - EC2 인스턴스에는 End-Of-Life 운영 체제가 있습니다.
  - EC2 인스턴스에 악성 소프트웨어 패키지가 있음
  - EC2 인스턴스에 악성 파일이 있음
- EC2 인스턴스의 영향 특성
  - 전체 제어 권한 있는 실행기 경로 보유
  - 직접 정책 에스컬레이션 경로가 있음
  - 신뢰 정책 하이재크 경로가 있음
  - 데이터 랜섬웨어 경로가 있음
  - 제한 경로 제거
  - 패스 역할 생성 실행기 경로가 있음
  - 스왑 역할 기존 실행기 경로가 있음
  - 역할 체인 에스컬레이션 경로가 있음
  - 코드 삽입 권한이 있는 실행기 경로가 있음
  - 감사 추적 경로 비활성화
  - 기존 실행기 경로에 액세스할 수 있음
  - 자격 증명 마이닝 경로가 있음
  - 전달 역할 데이터 액세스 경로가 있음
  - 역할 전달 작업 하이잭 경로가 있음
  - 단일 홉 데이터 액세스 경로가 있음
  - 기능 발전 경로가 있음

EC2 인스턴스의 잘못된 구성 특성

다음은 EC2 인스턴스의 잘못된 구성 특성 및 제안된 문제 해결 단계입니다.

EC2 인스턴스는 버전 1을 사용하여 IMDS에 대한 액세스를 허용합니다.

인스턴스 메타데이터는 애플리케이션이 실행 중인 인스턴스를 구성 또는 관리하는 데 사용될 수 있는 Amazon EC2 인스턴스에 대한 데이터입니다. 인스턴스 메타데이터 서비스(IMDS)는 인스턴스의 코드가 인스턴스 메타데이터에 안전하게 액세스하기 위해 사용하는 온 인스턴스 구성 요소입니다. IMDS는 제대로 보호되지 않을 경우 임시 자격 증명 및 기타 민감한 구성 데이터에 대한 액세스를 제공하므

로 잠재적인 공격 벡터가 될 수 있습니다. IMDSv2는 메타데이터 요청에 세션 토큰을 요구하고 세션 기간을 제한하는 세션 기반 인증을 통해 악용에 대한 더 강력한 보호를 제공합니다. 표준 보안 원칙에 따라 IMDSv2를 사용하고 IMDSv1을 비활성화하도록 Amazon EC2 인스턴스를 구성합니다. IMDSv2 IMDSv1

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

애플리케이션 호환성 테스트

IMDSv2를 구현하기 전에 인스턴스를 테스트하여 IMDSv2와의 호환성을 확인합니다. 일부 애플리케이션 또는 스크립트는 핵심 기능에 IMDSv1이 필요하고 추가 구성이 필요할 수 있습니다. 애플리케이션 호환성을 테스트하기 위한 도구 및 권장 경로에 대한 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 인스턴스 메타데이터 서비스 버전 2 사용으로 전환을 참조하세요.

IMDSv2를 사용하도록 인스턴스 업데이트

IMDSv2를 사용하도록 기존 인스턴스를 수정합니다. 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 기존 인스턴스에 대한 인스턴스 메타데이터 옵션 수정을 참조하세요.

Auto Scaling 그룹의 인스턴스에 업데이트 적용

인스턴스가 Auto Scaling 그룹에 속하는 경우 시작 템플릿 또는 시작 구성을 새 구성으로 업데이트하고 인스턴스 새로 고침을 수행합니다.

Amazon EC2 인스턴스에는 SSH 또는 RDP 액세스를 허용하는 보안 그룹 또는 네트워크 ACL이 있습니다

SSH 및 RDP와 같은 원격 액세스 프로토콜을 사용하면 사용자가 외부 위치에서 Amazon EC2 인스턴스에 연결하고 관리할 수 있습니다. 보안 그룹이 인터넷에서 이러한 프로토콜에 대한 무제한 액세스를 허용하면 인스턴스에 대한 인터넷 액세스가 가능하여 Amazon EC2 인스턴스의 공격 표면이 증가합니다. 표준 보안 원칙에 따라 신뢰할 수 있는 특정 IP 주소 또는 범위로 원격 액세스를 제한합니다.

문제 해결: 보안 그룹 규칙 수정

Amazon EC2 인스턴스에 대한 액세스를 신뢰할 수 있는 특정 IP 주소로 제한합니다. SSH 및 RDP 액세스를 신뢰할 수 있는 특정 IP 주소로 제한하거나 CIDR 표기법을 사용하여 IP 범위(예: 192.168.1.0/24)를 지정합니다. 보안 그룹 규칙을 수정하려면 Amazon Elastic Compute Cloud 사용 설명서의 보안 그룹 규칙 구성을 참조하세요.

Amazon EC2 인스턴스에 개방형 보안 그룹이 있음

보안 그룹은 Amazon EC2 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. 모든 IP 주소로부터 무제한 액세스를 허용하는 개방형 보안 그룹은 인스턴스를 무단 액세스에 노출시킬 수 있습니다. 표준 보안 원칙에 따라 보안 그룹 액세스를 특정 IP 주소 및 포트로 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

보안 그룹 규칙 검토 및 현재 구성 평가

`(0.0.0.0/0 or ::/0)`과 같은 광범위한 IP 범위에서 액세스할 수 있는 개방 포트를 평가합니다. 보안 그룹 세부 정보를 보는 방법에 대한 지침은 Porting Assistant for .NET API 참조의 DescribeSecurityGroups를 참조하세요.

보안 그룹 규칙 수정

보안 그룹 규칙을 수정하여 액세스를 신뢰할 수 있는 특정 IP 주소 또는 범위로 제한합니다. 보안 그룹 규칙을 업데이트할 때는 각 필수 소스 IP 범위에 대한 규칙을 생성하거나 특정 포트에 대한 액세스를 제한하여 네트워크 세그먼트마다 액세스 요구 사항을 분리하는 것이 좋습니다. 보안 그룹 규칙을 수정하려면 Amazon EC2 사용 설명서의 보안 그룹 규칙 구성을 참조하세요.

EC2 인스턴스의 연결성 특성

다음은 EC2 인스턴스의 연결성 특성 및 제안된 문제 해결 단계입니다.

EC2 인스턴스는 인터넷을 통해 연결할 수 있습니다

인터넷에서 연결할 수 있는 포트가 있는 Amazon EC2 인스턴스는 인스턴스를 노출할 수 있습니다. 연결성은 인터넷 게이트웨이(Application Load Balancer 또는 Classic Load Balancer 뒤에 있는 인스턴스 포함), VPC 피어링 연결 또는 VPN 가상 게이트웨이를 통해 발생할 수 있습니다. 표준 보안 원칙에 따라 인바운드 트래픽을 필요한 소스 및 포트로만 제한하여 최소 권한 네트워크 액세스 제어를 구현합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

보안 그룹 규칙 수정 또는 제어

리소스 탭에서 Amazon EC2 보안 그룹의 리소스를 엽니다. 인스턴스가 작동하는 데 인터넷 액세스가 필요한지 검토합니다. 무제한 액세스(`0.0.0.0/0` 또는 `::/0`)를 허용하는 인바운드 보안 그룹 규칙을 수정하거나 제거합니다. 특정 IP 범위 또는 보안 그룹을 기반으로 보다 제한적인 규칙을 구현합니다. 제한된 퍼블릭 액세스가 필요한 경우 인스턴스의 기능에 필요한 특정 포트 및 프로토콜로 액세스를 제한합니다. 보안 그룹 규칙 관리에 대한 지침은 Amazon EC2 사용 설명서의 보안 그룹 규칙 구성을 참조하세요.

네트워크 ACL 업데이트

인스턴스의 서브넷과 연결된 네트워크 액세스 제어 목록(ACL)을 검토하고 수정합니다. ACL 설정이 보안 그룹 변경 사항과 일치하고 의도치 않게 퍼블릭 액세스를 허용하지 않는지 확인합니다. 네트워크 ACL 수정에 대한 지침은 Amazon VPC 사용 설명서의 네트워크 ACL 작업을 참조하세요.

대체 액세스 방법

대체 액세스 방법에 대해 다음 옵션을 고려하세요.

- 아웃바운드 인터넷 연결에 NAT 게이트웨이 사용 - 인터넷에 액세스해야 하는 프라이빗 서브넷의 인스턴스(예: 업데이트 다운로드)의 경우 퍼블릭 IP 주소를 할당하는 대신 NAT 게이트웨이를 사용하는 것이 좋습니다. NAT 게이트웨이를 사용하면 프라이빗 서브넷의 인스턴스가 인터넷으로의 아웃바운드 연결을 시작하는 동시에 인터넷으로부터의 인바운드 연결을 방지할 수 있습니다.
- Systems Manager Session Manager 사용 - Session Manager는 인바운드 포트, SSH 키 관리 또는 배스천 호스트 유지 관리 없이 Amazon EC2 인스턴스에 대한 보안 쉘 액세스를 제공합니다.
- WAF 및 Elastic Load Balancing 또는 Application Load Balancer 사용 - 웹 애플리케이션을 실행하는 인스턴스의 경우 AWS 웹 애플리케이션 방화벽(WAF)과 결합된 LB를 사용하는 것이 좋습니다. 인스턴스가 프라이빗 서브넷에서 실행되는 동안 LB가 퍼블릭 서브넷에서 실행되어 인터넷 트래픽을 처리하도록 LB를 구성할 수 있습니다. 로드 밸런서에 WAF를 추가하면 웹 악용 및 봇에 대한 추가 보호 기능이 제공됩니다.

EC2 인스턴스의 취약성 특성

다음은 EC2 인스턴스의 취약성 특성 및 제안된 문제 해결 단계입니다.

EC2 인스턴스에 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있음

EC2 인스턴스에 설치된 소프트웨어 패키지는 일반 취약성 및 노출(CVE)에 노출될 수 있습니다. 중요 CVEs AWS 환경에 심각한 보안 위험을 초래합니다. 권한이 없는 위탁자는 이러한 패치되지 않은 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습

니다. 악용 가능성이 높은 심각한 취약성은 악용 코드가 이미 공개되어 있고 공격자 또는 자동 스캔 도구가 이를 적극적으로 사용할 수 있으므로 즉각적인 보안 위협을 나타냅니다. 이러한 취약성을 패치하여 인스턴스를 보호합니다.

문제 해결: 영향을 받는 인스턴스 업데이트

특성의 취약성 탭에서 참조 섹션을 검토합니다. 공급업체 설명서에는 특정 문제 해결 지침이 포함될 수 있습니다. 다음 일반 지침을 사용하여 적절한 문제 해결을 따르세요.

Systems Manager Patch Manager를 사용하여 운영 체제와 애플리케이션 모두에 패치를 적용합니다. Patch Manager는 대규모 인스턴스 그룹에서 운영 체제 및 소프트웨어 패치를 자동으로 선택하고 배포하는 데 도움이 됩니다. 패치 관리자를 구성하지 않은 경우 영향을 받는 각 인스턴스에서 운영 체제를 수동으로 업데이트합니다.

공급업체의 권장 절차에 따라 영향을 받는 애플리케이션을 최신 보안 버전으로 업데이트합니다. 여러 인스턴스에서 애플리케이션 업데이트를 관리하려면 Systems Manager State Manager를 사용하여 소프트웨어를 일관된 상태로 유지하는 것이 좋습니다. 업데이트를 사용할 수 없는 경우 패치가 릴리스되거나 애플리케이션에 대한 네트워크 액세스 제한 또는 취약한 기능 비활성화와 같은 기타 완화 조치가 있을 때까지 취약한 애플리케이션을 제거하거나 비활성화하는 것이 좋습니다.

Amazon Inspector 조사 결과에 제공된 특정 문제 해결 조언을 따릅니다. 여기에는 보안 그룹 규칙 변경, 인스턴스 구성 수정 또는 애플리케이션 설정 조정이 포함될 수 있습니다.

인스턴스가 Auto Scaling 그룹의 일부인지 확인합니다. AMI 교체 패치는 Auto Scaling 그룹에 새 Amazon EC2 인스턴스를 배포하도록 구성된 AMI ID를 업데이트하여 변경 불가능한 인프라에서 수행됩니다. 사용자 지정/골든 AMI를 사용하는 경우 새 AMI로 인스턴스를 생성한 다음 인스턴스를 사용자 지정하고 새 골든 AMI를 생성합니다. 자세한 내용은 AMI 업데이트 패치 적용(Auto Scaling 그룹에 패치된 AMI 사용)을 참조하세요.

향후 고려 사항

향후 취약성 발생을 방지하려면 취약성 관리 프로그램을 구현하는 것이 좋습니다. 인스턴스에서 CVE를 자동으로 스캔하도록 Amazon Inspector를 구성할 수 있습니다. 또한 자동 문제 해결을 위해 Amazon Inspector를 Security Hub와 통합할 수도 있습니다. 인스턴스 중단을 최소화하려면 Systems Manager Maintenance Windows를 사용하여 정기적인 패치 적용 일정을 구현하는 것이 좋습니다.

Amazon EC2 인스턴스에 소프트웨어 취약성이 있음

Amazon EC2 인스턴스에 설치된 소프트웨어 패키지는 일반적인 취약성 및 노출(CVEs. 비중요 CVE는 중요 CVE에 비해 심각도 또는 악용 가능성이 낮은 보안 약점을 나타냅니다. 이러한 취약점은 즉각적

인 위험을 초래하지는 않지만, 공격자는 이러한 패치되지 않은 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습니다. 보안 모범 사례에 따라 이러한 취약성을 패치하여 공격으로부터 인스턴스를 보호합니다.

문제 해결: 영향을 받는 인스턴스 업데이트

AWS Systems Manager Patch Manager를 사용하여 운영 체제에 패치를 적용합니다. Patch Manager는 대규모 인스턴스 그룹에서 운영 체제 및 소프트웨어 패치를 자동으로 선택하고 배포하는 데 도움이 됩니다. 패치 관리자를 구성하지 않은 경우 영향을 받는 각 인스턴스에서 운영 체제를 수동으로 업데이트합니다.

공급업체의 권장 절차에 따라 영향을 받는 애플리케이션을 최신 보안 버전으로 업데이트합니다. 여러 인스턴스에서 애플리케이션 업데이트를 관리하려면 AWS Systems Manager State Manager를 사용하여 소프트웨어를 일관된 상태로 유지하는 것이 좋습니다. 업데이트를 사용할 수 없는 경우 패치가 릴리스되거나 애플리케이션에 대한 네트워크 액세스 제한 또는 취약한 기능 비활성화와 같은 기타 완화 조치가 있을 때까지 취약한 애플리케이션을 제거하거나 비활성화하는 것이 좋습니다.

Amazon Inspector 조사 결과에 제공된 특정 문제 해결 조언을 따릅니다. 여기에는 보안 그룹 규칙 변경, 인스턴스 구성 수정 또는 애플리케이션 설정 조정이 포함될 수 있습니다.

인스턴스가 Auto Scaling 그룹의 일부인지 확인합니다. AMI 교체 패치는 Auto Scaling 그룹에 새 Amazon EC2 인스턴스를 배포하도록 구성된 AMI ID를 업데이트하여 변경 불가능한 인프라에서 수행됩니다. 사용자 지정/골든 AMI를 사용하는 경우 새 AMI로 인스턴스를 생성한 다음 인스턴스를 사용자 지정하고 새 골든 AMI를 생성합니다. 자세한 내용은 AMI 업데이트 패치 적용(Auto Scaling 그룹에 패치된 AMI 사용)을 참조하세요.

향후 고려 사항

향후 취약성 발생을 방지하려면 취약성 관리 프로그램을 구현하는 것이 좋습니다. 인스턴스에서 CVE를 자동으로 스캔하도록 Amazon Inspector를 구성할 수 있습니다. 또한 자동 문제 해결을 위해 Amazon Inspector를 Security Hub와 통합할 수도 있습니다. 인스턴스 중단을 최소화하려면 Systems Manager Maintenance Windows를 사용하여 정기적인 패치 적용 일정을 구현하는 것이 좋습니다.

EC2 인스턴스에는 End-Of-Life 운영 체제가 있습니다.

EC2 인스턴스는 원래 개발자가 더 이상 지원하거나 유지 관리하지 않는 end-of-life 운영 체제를 실행합니다. 이렇게 하면 인스턴스가 보안 취약성 및 잠재적 공격에 노출됩니다. 운영 체제end-of-life하면 공급업체는 일반적으로 새 보안 권고 릴리스를 중지합니다. 공급업체 피드에서 기존 보안 권고를 제거할 수도 있습니다. 따라서 Amazon InspectorCVEs에 대한 결과 생성을 잠재적으로 중지하여 보안 적용 범위에 추가 격차를 초래할 수 있습니다.

Amazon Inspector에서 감지할 수 있는 수명이 다한 운영 체제에 대한 자세한 내용은 Amazon Inspector 사용 설명서의 중단된 운영 체제를 참조하세요. Amazon Inspector

문제 해결: 지원되는 운영 체제 버전으로 업데이트

지원되는 운영 체제 버전으로 업데이트합니다. 노출 조사 결과에서 리소스를 열어 영향을 받는 리소스에 액세스합니다. 인스턴스에서 운영 체제 버전을 업데이트하기 전에 롤백해야 하는 경우를 대비하여 스냅샷 또는 AMI 백업을 생성합니다. 그런 다음 Amazon Inspector 사용 설명서의 지원되는 운영 체제에서 사용 가능한 버전을 검토하여 현재 지원되는 OS 버전 목록을 확인합니다.

EC2 인스턴스에 악성 소프트웨어 패키지가 있음

악성 패키지는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함된 소프트웨어 구성 요소입니다. 공격자가 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있기 때문에 악성 패키지는 인스턴스에 능동적이고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 패키지를 제거하여 잠재적 공격으로부터 인스턴스를 보호합니다.

문제 해결: 악성 패키지 제거

특성의 취약성 탭에 있는 참조 섹션에서 악성 패키지 세부 정보를 검토하여 위협을 이해합니다. 적절한 패키지 관리자를 사용하여 식별된 악성 패키지를 제거합니다. 예제는 Amazon Linux 2023 사용 설명서의 패키지 관리 도구를 참조하세요. 악성 패키지를 제거한 후에는 스캔을 수행하여 악성 코드에 의해 설치되었을 수 있는 모든 패키지가 제거되었는지 확인하는 것이 좋습니다. 자세한 내용은의 GuardDuty에서 온디맨드 맬웨어 스캔 시작을 참조하세요.

EC2 인스턴스에 악성 파일이 있음

악성 파일에는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함되어 있습니다. 공격자가 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있으므로 악성 파일은 인스턴스에 활성적이고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 파일을 제거하여 잠재적 공격으로부터 인스턴스를 보호합니다.

문제 해결: 악성 파일 제거

악성 파일이 있는 특정 Amazon Elastic Block Store(Amazon EBS) 볼륨을 식별하려면 특성의 결과 세부 정보의 리소스 섹션을 검토하세요. 악성 파일로 볼륨을 식별한 후 변경하기 전에 볼륨의 스냅샷을 생성한 다음 식별된 악성 파일을 제거합니다. 악성 파일을 제거한 후에는 스캔을 수행하여 악성 파일에 의해 설치되었을 수 있는 모든 파일이 제거되었는지 확인하는 것이 좋습니다. 자세한 내용은의 GuardDuty에서 온디맨드 맬웨어 스캔 시작을 참조하세요.

EC2 인스턴스의 영향 특성

영향 특성은 노출의 잠재적 폭발 반경을 설명합니다. Security Hub는 EC2 인스턴스와 연결된 AWS Identity and Access Management 보안 주체의 유효 권한을 분석하여 인스턴스가 손상된 경우 공격자가 도달할 수 있는 다운스트림 리소스를 결정합니다. 각 영향 특성은 특정 권한 에스컬레이션 패턴을 식별합니다. 블래스트 반경을 줄이려면 각 특성에 설명된 권한 경로를 검토하고 불필요한 권한을 제거합니다.

표준 보안 원칙에 따라 작업을 수행하는 데 필요한 권한만 제공하여 최소 권한을 부여합니다. 광범위한 정책을 필요한 특정 작업 및 리소스만 부여하는 범위 축소 정책으로 바꿉니다. 제거할 미사용 권한을 식별하려면 IAM Access Analyzer를 사용하여 액세스 기록을 기반으로 권장 사항을 생성합니다. 자세한 내용은 IAM 사용 설명서의 외부 및 미사용 액세스 결과 및 최소 권한 적용을 참조하세요.

전체 제어 권한 있는 실행기 경로 보유

연결된 보안 주체는 이미 승격된 권한이 있는 컴퓨팅 리소스에 역할을 전달하고 코드를 주입할 수 있습니다. 이를 통해 보안 주체는 실행기를 완전히 제어하고 실행기의 역할이 허용하는 모든 작업을 수행할 수 있습니다.

직접 정책 에스컬레이션 경로가 있음

연결된 보안 주체는 IAM 정책을 직접 수정하여 추가 권한을 부여하고 중간 리소스 없이 자체 권한을 에스컬레이션할 수 있습니다.

신뢰 정책 하이재크 경로가 있음

연결된 보안 주체는 IAM 역할의 신뢰 정책을 수정하여가 해당 역할을 수임하여 역할의 권한을 얻도록 허용할 수 있습니다.

데이터 랜섬웨어 경로가 있음

연결된 보안 주체는 고객 관리형 AWS KMS 키로 Amazon S3 객체를 암호화한 다음 키 정책을 수정하는 등 랜섬웨어에 사용할 수 있는 방식으로 데이터를 암호화하거나 삭제할 수 있습니다.

제한 경로 제거

연결된 보안 주체는 권한 경계, 서비스 제어 정책 또는 리소스 기반 정책 거부 문과 같은 보안 제한을 제거하여 다른 보안 주체 또는 리소스 자체가 수행할 수 있는 작업을 확장할 수 있습니다.

패스 역할 생성 실행기 경로가 있음

연결된 보안 주체는 새 컴퓨팅 리소스(예: Lambda 함수 또는 Amazon EC2 인스턴스)를 생성하고 권한 있는 역할을 전달하여 새 리소스를 통해 자체 권한을 효과적으로 로세싱할 수 있습니다.

스왑 역할 기존 실행기 경로가 있음

연결된 보안 주체는 기존 컴퓨팅 리소스에 연결된 IAM 역할을 변경하여 더 권한이 있는 역할로 대체하여 액세스를 에스컬레이션할 수 있습니다.

역할 체인 에스컬레이션 경로가 있음

연결된 보안 주체는 일련의 역할을 수임할 수 있습니다. 여기서 체인의 각 역할은 점진적으로 더 광범위한 권한을 가지므로 궁극적으로 권한이 높은 역할에 도달합니다.

코드 삽입 권한이 있는 실행기 경로가 있음

연결된 보안 주체는 권한이 승격된 실행 중인 컴퓨팅 리소스에 코드를 주입하여 해당 리소스의 권한 있는 역할에 따라 임의 작업을 실행할 수 있습니다.

감사 추적 경로 비활성화

연결된 보안 주체는 CloudTrail과 같은 로깅 또는 모니터링 서비스를 비활성화하여 에스컬레이션 중 또는 에스컬레이션 후에 트랙을 효과적으로 처리할 수 있습니다.

기존 실행기 경로에 액세스할 수 있음

연결된 보안 주체는 기존 컴퓨팅 리소스를 호출하거나 연결하고 연결된 역할을 사용하여 권한 있는 작업을 수행할 수 있습니다.

자격 증명 마이닝 경로가 있음

연결된 보안 주체는 다른 보안 주체에 대한 새 장기 자격 증명(예: 액세스 키 또는 로그인 프로필)을 생성하여 암호 교체 또는 세션 만료 후에도 지속되는 영구 액세스 경로를 설정할 수 있습니다.

전달 역할 데이터 액세스 경로가 있음

연결된 보안 주체는 서비스 리소스를 생성하고 민감한 데이터에 액세스할 수 있는 역할을 전달하여 새 리소스를 통해 해당 데이터에 간접적으로 액세스할 수 있습니다.

역할 전달 작업 하이잭 경로가 있음

연결된 보안 주체는 예약된 작업 또는 이벤트 기반 작업(예: 이벤트에 의해 트리거된 Lambda 함수)에 역할을 전달하여 해당 역할의 권한으로 임의 코드를 실행할 수 있습니다.

단일 홉 데이터 액세스 경로가 있음

연결된 보안 주체는 중간 에스컬레이션 단계 없이 기존 권한을 통해 민감한 데이터 리소스(예: Amazon S3 버킷 또는 DynamoDB 테이블)에 직접 액세스할 수 있습니다.

기능 발전 경로가 있음

연결된 보안 주체에는 직접 할당된 권한 이상으로 전체 기능을 발전시키는 권한 에스컬레이션 경로가 있습니다. 이는 보다 구체적인 패턴과 일치하지 않는 경로에 대한 일반적인 분류입니다.

## Amazon ECS 서비스에 대한 노출 문제 해결

AWS Security Hub는 Amazon Elastic Container Service(Amazon ECS) 서비스에 대한 노출 조사 결과를 생성할 수 있습니다.

노출 조사 결과와 관련된 Amazon ECS 서비스 및 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 이러한 리소스 세부 정보는 Security Hub 콘솔에서 검색하거나 Security Hub CSPM API의 GetFindingsV2 작업을 통해 프로그래밍 방식으로 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침은 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Amazon ECS 서비스의 잘못된 구성 특성
  - Amazon ECS 서비스에서 컨테이너가 루트 파일 시스템에 액세스할 수 있도록 허용하는 태스크 정의를 사용
  - Amazon ECS 서비스에서 호스트의 프로세스 네임스페이스를 공유하도록 구성된 태스크 정의를 사용
  - Amazon ECS 서비스가 환경 변수에서 일반 텍스트 자격 증명으로 구성된 태스크 정의를 사용
  - Amazon ECS 서비스에 개방형 보안 그룹이 있음
  - Amazon ECS 서비스에는 퍼블릭 IP 주소가 있습니다.

  - Amazon ECS 서비스에서 호스트 네트워킹 모드가 활성화된 상태로 구성된 태스크 정의를 사용
- Amazon ECS 서비스의 연결성 특성
  - Amazon ECS 서비스는 인터넷을 통해 연결할 수 있습니다.
- Amazon ECS 서비스의 취약성 특성
  - Amazon ECS 서비스에 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있는 컨테이너가 있음
  - Amazon ECS 서비스에 소프트웨어 취약성이 있는 컨테이너가 있음
  - Amazon ECS 서비스에는 End-Of-Life 운영 체제가 있는 컨테이너가 있습니다.
  - Amazon ECS 서비스에는 악성 소프트웨어 패키지가 있는 컨테이너가 있습니다.
- Amazon ECS 서비스의 영향 특성
  - 전체 제어 권한 있는 실행기 경로 보유
  - 직접 정책 에스컬레이션 경로가 있음
  - 신뢰 정책 하이재크 경로가 있음
  - 데이터 랜섬웨어 경로가 있음
  - 제한 경로 제거
  - 패스 역할 생성 실행기 경로가 있음
  - 스왑 역할 기존 실행기 경로가 있음
  - 역할 체인 에스컬레이션 경로가 있음
  - 코드 삽입 권한이 있는 실행기 경로가 있음
  - 감사 추적 경로 비활성화
  - 기존 실행기 경로에 액세스할 수 있음
  - 자격 증명 마이닝 경로가 있음
  - 전달 역할 데이터 액세스 경로가 있음
  - 역할 전달 작업 하이잭 경로가 있음
  - 단일 홉 데이터 액세스 경로가 있음
  - 기능 발전 경로가 있음

### Amazon ECS 서비스의 잘못된 구성 특성

다음은 Amazon ECS 서비스의 잘못된 구성 특성 및 제안된 문제 해결 단계입니다.

### Amazon ECS 서비스에서 컨테이너가 루트 파일 시스템에 액세스할 수 있도록 허용하는 태스크 정의를 사용

호스트 루트 파일 시스템에 액세스할 수 있는 Amazon ECS 컨테이너는 잠재적으로 호스트 시스템에서 중요한 파일을 읽거나 수정하거나 실행할 수 있습니다. 이러한 구성은 손상된 컨테이너가 의도한 범위를 벗어난 리소스에 액세스하거나 수정하는 데 사용될 위험을 증가시켜 호스트 파일 시스템의 민감한 데이터가 노출이 발생할 수 있습니다. 표준 보안 원칙에 따라 최소 권한을 부여합니다. 즉, 작업을 수행하는 데 필요한 권한만 부여합니다.

해결 방법: 호스트 파일 시스템 액세스 권한이 있는 컨테이너 검토 및 수정

노출 조사 결과에서 태스크 정의 ARN을 식별합니다. 새 Amazon ECS 콘솔에서 태스크 정의를 엽니다. 태스크 정의에서 호스트 경로 매핑을 정의하는 볼륨 섹션을 찾습니다.

태스크 정의를 검토하여 컨테이너 기능에 호스트 파일 시스템 액세스가 필요한지 확인합니다. 호스트 파일 시스템 액세스가 필요하지 않은 경우 태스크 정의를 수정하여 호스트 경로를 사용하는 볼륨 정의를 모두 제거합니다. 호스트 파일 시스템 액세스가 필요한 경우 무단 수정을 방지하기 위해 읽기 전용 파일 시스템을 사용하도록 컨테이너를 구성하는 것이 좋습니다.

### Amazon ECS 서비스에서 호스트의 프로세스 네임스페이스를 공유하도록 구성된 태스크 정의를 사용

노출된 네임스페이스로 실행되는 Amazon ECS 컨테이너는 호스트 시스템 리소스 및 기타 컨테이너 네임스페이스에 액세스할 수 있습니다. 이 구성을 사용하면 손상된 컨테이너가 격리 경계를 벗어나 프로세스, 네트워크 인터페이스 또는 기타 리소스에 의도한 범위를 벗어나게 할 수 있습니다.

프로세스 ID(PID) 네임스페이스는 프로세스 간 분리를 제공합니다. 시스템 프로세스가표시되는 것을 방지하고 PID 1을 포함한 PID를 재사용할 수 있습니다. 호스트 PID 네임스페이스가 컨테이너와 공유되는 경우 컨테이너는 호스트 시스템의 모든 프로세스를 볼 수 있으므로 프로세스 수준 격리가 줄어듭니다. 이로 인해 호스트 프로세스를 조작하고 종료하는 기능을 포함하여 호스트 프로세스에 대한 무단 액세스가 발생할 수 있습니다. 표준 보안 원칙에 따라 컨테이너에 대한 적절한 네임스페이스 격리를 유지합니다.

문제 해결: 네임스페이스가 노출된 태스크 정의 업데이트

노출의 리소스 탭을 열고 노출된 네임스페이스가 있는 태스크 정의를 식별합니다. 새 Amazon ECS 콘솔에서 태스크 정의를 엽니다. 호스트와 프로세스 ID 네임스페이스를 공유하는 호스트 값을 가진 pidMode 설정을 찾습니다. 태스크 정의에서 pidMode: 호스트 설정을 제거하여 컨테이너가 적절한 네임스페이스 격리로 실행되도록 합니다.

Amazon ECS 서비스가 환경 변수에서 일반 텍스트 자격 증명으로 구성된 태스크 정의를 사용

환경 변수에 일반 텍스트 자격 증명이 있는 Amazon ECS 컨테이너는 공격자가 태스크 정의, 컨테이너 환경 또는 컨테이너 로그에 액세스할 경우 손상될 수 있는 민감한 인증 정보를 노출합니다. 이렇게 하면 유출된 자격 증명을 사용하여 다른 AWS 서비스 또는 리소스에 액세스할 수 있으므로 상당한 보안 위험이 발생합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

일반 텍스트 자격 증명 교체

노출 조사 결과에서 일반 텍스트 자격 증명을 사용하는 태스크 정의를 식별합니다. 새 Amazon ECS 콘솔에서 태스크 정의를 엽니다. 컨테이너 정의에서 AWS 액세스 키, 데이터베이스 암호, API 토큰과 같은 민감한 값을 포함하는 환경 변수를 찾습니다.

자격 증명 전달하려면 다음 대안을 고려하세요.

- AWS 액세스 키를 사용하는 대신 IAM 작업 실행 역할 및 작업 역할을 사용하여 컨테이너에 권한을 부여합니다.
- 자격 증명을에 보안 암호로 저장 AWS Secrets Manager 하고 작업 정의에서 참조합니다.

작업 정의 업데이트

자격 증명을 안전하게 처리하도록 수정한 새 태스크 정의를 생성합니다. 그런 다음 새로 수정한 태스크 정의를 사용하도록 Amazon ECS 서비스를 업데이트합니다.

Amazon ECS 서비스에 개방형 보안 그룹이 있음

보안 그룹은 Amazon ECS 태스크에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. 모든 IP 주소로부터 무제한 액세스를 허용하는 개방형 보안 그룹은 컨테이너를 무단 액세스에 노출시켜 자동 스캔 도구 및 표적 공격에 노출될 위험을 증가시킬 수 있습니다. 표준 보안 원칙에 따라 보안 그룹 액세스를 특정 IP 주소 및 포트로 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

보안 그룹 규칙 검토 및 현재 구성 평가

Amazon ECS 보안 그룹의 리소스를 엽니다. (`0.0.0.0/0 or ::/0`)과 같은 광범위한 IP 범위에서 액세스할 수 있는 개방 포트를 평가합니다.

보안 그룹 규칙 수정

보안 그룹 규칙을 수정하여 액세스를 신뢰할 수 있는 특정 IP 주소 또는 범위로 제한합니다. 보안 그룹 규칙을 업데이트할 때는 각 필수 소스 IP 범위에 대한 규칙을 생성하거나 특정 포트에 대한 액세스를 제한하여 네트워크 세그먼트마다 액세스 요구 사항을 분리하는 것이 좋습니다.

보안 그룹 규칙 수정

대체 액세스 방법에 대해 다음 옵션을 고려하세요.

- Session Manager는 인바운드 포트, SSH 키 관리 또는 배스천 호스트 유지 관리 없이 Amazon EC2 인스턴스에 대한 보안 쉘 액세스를 제공합니다.
- NACL은 서브넷 수준에서 추가 보안 계층을 제공합니다. 보안 그룹과 달리 NACL은 상태 비저장이며 인바운드 및 아웃바운드 규칙을 모두 명시적으로 정의해야 합니다.

Amazon ECS 서비스에는 퍼블릭 IP 주소가 있습니다.

태스크에 퍼블릭 IP 주소가 할당된 Amazon ECS 서비스는 인터넷에서 직접 액세스할 수 있습니다. 이는 공개적으로 사용 가능해야 하는 서비스에 필요할 수 있지만 공격 표면과 무단 액세스 가능성을 높입니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

퍼블릭 IP 주소를 사용하는 서비스 식별

노출 조사 결과에서 태스크에 퍼블릭 IP 주소가 할당된 Amazon ECS 서비스를 식별합니다. 서비스 구성에서 값이 `ENABLED`인 `assignPublicIp` 설정을 찾습니다.

작업 정의 업데이트

퍼블릭 IP 주소를 비활성화하도록 수정한 새 태스크 정의를 생성합니다. 그런 다음 새로 수정한 태스크 정의를 사용하도록 Amazon ECS 서비스를 업데이트합니다.

프라이빗 네트워크 액세스 패턴 구현

웹 애플리케이션을 실행하는 인스턴스의 경우 로드 밸런서(LB)를 사용하는 것이 좋습니다. 인스턴스가 프라이빗 서브넷에서 실행되는 동안 LB가 퍼블릭 서브넷에서 실행되어 인터넷 트래픽을 처리하도록 LB를 구성할 수 있습니다.

Amazon ECS 서비스에서 호스트 네트워킹 모드가 활성화된 상태로 구성된 태스크 정의를 사용

호스트 네트워킹 모드로 실행되는 Amazon ECS 컨테이너는 네트워크 네임스페이스를 호스트와 공유하므로 호스트의 네트워크 인터페이스, 포트 및 라우팅 테이블에 직접 액세스할 수 있습니다. 이러한 구성은 컨테이너가 제공하는 네트워크 격리를 우회하여 컨테이너에서 실행되는 서비스를 외부 네트워크에 직접 노출하고 컨테이너가 호스트 네트워크 설정을 수정할 수 있도록 합니다. 표준 보안 원칙에 따라 컨테이너에 대한 적절한 네트워크 격리를 유지합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

호스트 네트워킹 모드 비활성화

노출 조사 결과에서 호스트 네트워킹 모드를 사용하는 태스크 정의를 식별합니다. 새 Amazon ECS 콘솔에서 태스크 정의를 엽니다. 태스크 정의에서 호스트 값이 있는 networkMode 설정을 찾습니다.

호스트 네트워킹 모드를 비활성화하려면 다음 옵션을 고려합니다.

- `awsvpc` 네트워크 모드는 각 태스크에 고유한 탄력적 네트워크 인터페이스를 제공하여 가장 강력한 수준의 네트워크 격리를 제공합니다.
- `bridge` 네트워크 모드는 포트 매핑이 특정 컨테이너 포트를 호스트에 노출하도록 허용하면서 격리를 제공합니다.

작업 정의 업데이트

업데이트된 네트워크 모드 구성을 사용하여 새 태스크 정의를 생성합니다. 그런 다음 새로 수정한 태스크 정의를 사용하도록 Amazon ECS 서비스를 업데이트합니다.

Amazon ECS 서비스의 연결성 특성

다음은 Amazon ECS 서비스의 접근성 특성과 제안된 문제 해결 단계입니다.

Amazon ECS 서비스는 인터넷을 통해 연결할 수 있습니다.

퍼블릭 서브넷에서 작업을 실행하는 Amazon ECS 서비스는 인터넷에서 직접 액세스할 수 있습니다. 이렇게 하면 공격 표면과 무단 액세스 위험이 증가합니다. 표준 보안 원칙에 따라 프라이빗 서브넷에서 작업을 실행하고 서비스에 필요한 인터넷 액세스만 허용합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

프라이빗 서브넷에서 작업 실행

작업을 퍼블릭 서브넷에서 이동하려면 시작 유형에 대한 네트워크 구성을 업데이트합니다.

- Fargate의 경우 Amazon ECS 서비스의 네트워크 구성에 프라이빗 서브넷을 지정하고를 `assignPublicIp`로 설정합니다`DISABLED`. Amazon ECS는 프라이빗 서브넷에서 각 작업을 호스팅하고 서브넷과 연결된 NAT 게이트웨이를 통해 아웃바운드 트래픽을 라우팅합니다.
- EC2의 경우 프라이빗 서브넷에서 클러스터 용량을 제공하는 컨테이너 인스턴스를 시작합니다. 작업은 호스트의 프라이빗 네트워킹을 사용하고 NAT 게이트웨이를 통해 아웃바운드 트래픽을 라우팅합니다.

아웃바운드 액세스에 NAT 게이트웨이 사용

아웃바운드 인터넷 액세스가 필요한 프라이빗 서브넷의 작업의 경우 NAT 게이트웨이를 사용합니다. NAT 게이트웨이를 사용하여 태스크가 인터넷에 대한 아웃바운드 연결을 시작하고 인터넷으로부터의 인바운드 연결을 방지하도록 할 수 있습니다. 자세한 내용은 Amazon ECS 개발자 안내서의 인터넷에 Amazon ECS 애플리케이션 연결을 참조하세요.

인바운드 액세스에 로드 밸런서 사용

인터넷 트래픽을 수락해야 하는 서비스의 경우 퍼블릭 서브넷에서 실행되는 로드 밸런서 뒤의 프라이빗 서브넷에서 작업을 실행합니다. 웹 악용 및 봇에 대한 보호를 추가하려면 AWS Web Application Firewall(WAF)을 로드 밸런서와 연결합니다. 자세한 내용은 Amazon ECS 개발자 안내서의 로드 밸런싱을 사용하여 Amazon ECS 서비스 트래픽 분산을 참조하세요.

Amazon ECS 서비스의 취약성 특성

다음은 Amazon ECS의 취약성 특성 및 제안된 문제 해결 단계입니다.

Amazon ECS 서비스에 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있는 컨테이너가 있음

1. 노출 이해

   패키지 취약성 조사 결과는 사용자 AWS 환경에서 일반적인 취약성 및 노출(CVE)에 표시된 소프트웨어 패키지를 식별합니다. 공격자는 이러한 패치되지 않은 취약성을 악용하여 데이터의 기밀성, 무

결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습니다. ECR 컨테이너 이미지에는 패키지 취약성 조사 결과가 있을 수 있습니다.

2. 노출 문제 해결

   a. 패키지 버전 업데이트

      ECR 컨테이너 이미지의 패키지 취약성 조사 결과를 검토합니다. Amazon Inspector에서 제안한 대로 패키지 버전을 업데이트합니다. 자세한 내용은 Amazon Inspector 사용 설명서의 Amazon Inspector 조사 결과에 대한 세부 정보 보기를 참조하세요. Amazon Inspector 콘솔에서 조사 결과 세부 정보의 문제 해결 섹션에 패키지를 업데이트하기 위해 실행할 수 있는 명령이 표시됩니다.

   b. 기본 컨테이너 이미지 업데이트

      기본 컨테이너 이미지를 정기적으로 재구축하고 업데이트하여 컨테이너를 최신 상태로 유지합니다. 이미지를 다시 빌드할 때 공격 표면을 줄이기 위해 불필요한 구성 요소를 포함하지 마십시오. 컨테이너 이미지 재구축에 대한 지침은 Rebuild your images often을 참조하세요.

Amazon ECS 서비스에 소프트웨어 취약성이 있는 컨테이너가 있음

Amazon ECS 컨테이너에 설치된 소프트웨어 패키지는 일반 취약성 및 노출(CVE)에 노출될 수 있습니다. 우선순위가 낮은 취약성은 우선순위가 높은 취약성에 비해 심각도 또는 악용 가능성이 낮은 보안 약점을 나타냅니다. 이러한 취약성은 즉각적인 위험을 초래하지 않지만 공격자는 패치되지 않은 이러한 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

영향을 받는 컨테이너 이미지 업데이트

특성의 취약성 탭에서 참조 섹션을 검토합니다. 공급업체 설명서에는 특정 문제 해결 지침이 포함될 수 있습니다.

다음 일반 지침에 따라 적절한 문제 해결을 적용합니다.

- 영향을 받는 패키지의 패치 버전을 사용하도록 컨테이너 이미지를 업데이트합니다.
- 애플리케이션에서 영향을 받는 종속성을 안전한 최신 버전으로 업데이트합니다.

컨테이너 이미지를 업데이트한 후 컨테이너 레지스트리로 푸시하고 새 이미지를 사용하도록 Amazon ECS 태스크 정의를 업데이트합니다.

향후 고려 사항

컨테이너 이미지의 보안 태세를 더욱 강화하려면 Amazon ECS 태스크 및 컨테이너 보안 모범 사례를 따르는 것이 좋습니다. 컨테이너에서 CVE를 자동으로 스캔하도록 Amazon Inspector를 구성할 수 있습니다. 또한 자동 문제 해결을 위해 Amazon Inspector를 Security Hub와 통합할 수도 있습니다. 컨테이너 중단을 최소화하려면 Systems Manager Maintenance Windows를 사용하여 정기적인 패치 적용 일정을 구현하는 것이 좋습니다.

Amazon ECS 서비스에는 End-Of-Life 운영 체제가 있는 컨테이너가 있습니다.

Amazon ECS 컨테이너는 원래 개발자가 더 이상 지원하거나 유지 관리하지 않는 end-of-life 운영 체제를 사용합니다. 이렇게 하면 컨테이너가 보안 취약성 및 잠재적 공격에 노출됩니다. 운영 체제end-of-life하면 공급업체는 일반적으로 새로운 보안 권고 릴리스를 중지합니다. 공급업체 피드에서 기존 보안 권고를 제거할 수도 있습니다. 따라서 Amazon InspectorCVEs에 대한 결과 생성을 잠재적으로 중지하여 보안 적용 범위에 추가 격차를 초래할 수 있습니다.

Amazon Inspector에서 감지할 수 있는 수명이 다한 운영 체제에 대한 자세한 내용은 Amazon Inspector 사용 설명서의 중단된 운영 체제를 참조하세요. Amazon Inspector

문제 해결: 지원되는 운영 체제 버전으로 업데이트

지원되는 운영 체제 버전으로 업데이트합니다. 노출 조사 결과에서 리소스를 열어 영향을 받는 리소스에 액세스합니다. 컨테이너 이미지에서 운영 체제 버전을 업데이트하기 전에 현재 지원되는 OS 버전 목록은 Amazon Inspector 사용 설명서의 지원되는 운영 체제에서 사용 가능한 버전을 검토하세요. Amazon Inspector  컨테이너 이미지를 업데이트한 후 컨테이너 레지스트리로 푸시하고 새 이미지를 사용하도록 Amazon ECS 태스크 정의를 업데이트합니다.

Amazon ECS 서비스에는 악성 소프트웨어 패키지가 있는 컨테이너가 있습니다.

악성 패키지는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함된 소프트웨어 구성 요소입니다. 공격자가 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있기 때문에 악성 패키지는 Amazon ECS 컨테이너 이미지에 능동적이고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 패키지를 제거하여 잠재적 공격으로부터 컨테이너를 보호합니다.

문제 해결: 악성 패키지 제거

특성의 취약성 탭에 있는 참조 섹션에서 악성 패키지 세부 정보를 검토하여 위협을 이해합니다. 컨테이너 이미지에서 식별된 악성 패키지를 제거한 다음 다시 빌드합니다. 자세한 내용은 Amazon ECS API 참조의 ContainerDependency를 참조하세요. AWS

컨테이너 이미지를 업데이트한 후 컨테이너 레지스트리로 푸시하고 새 이미지를 사용하도록 Amazon ECS 태스크 정의를 업데이트합니다. 자세한 내용은 Amazon ECS 개발자 안내서의 콘솔을 사용하여 Amazon ECS 태스크 정의 업데이트를 참조하세요. AWS

Amazon ECS 서비스의 영향 특성

영향 특성은 노출의 잠재적 폭발 반경을 설명합니다. Security Hub는 Amazon ECS 서비스와 연결된 AWS Identity and Access Management 보안 주체의 유효 권한을 분석하여 서비스가 손상된 경우 공격자가 도달할 수 있는 다운스트림 리소스를 결정합니다. 각 영향 특성은 특정 권한 에스컬레이션 패턴을 식별합니다. 블래스트 반경을 줄이려면 각 특성에 설명된 권한 경로를 검토하고 불필요한 권한을 제거합니다.

표준 보안 원칙에 따라 작업을 수행하는 데 필요한 권한만 제공하여 최소 권한을 부여합니다. 광범위한 정책을 필요한 특정 작업 및 리소스만 부여하는 범위 축소 정책으로 바꿉니다. 제거할 미사용 권한을 식별하려면 IAM Access Analyzer를 사용하여 액세스 기록을 기반으로 권장 사항을 생성합니다. 자세한 내용은 IAM 사용 설명서의 외부 및 미사용 액세스 결과 및 최소 권한 적용을 참조하세요.

전체 제어 권한 있는 실행기 경로 보유

연결된 보안 주체는 이미 승격된 권한이 있는 컴퓨팅 리소스에 역할을 전달하고 코드를 주입할 수 있습니다. 이를 통해 보안 주체는 실행기를 완전히 제어하고 실행기의 역할이 허용하는 모든 작업을 수행할 수 있습니다.

직접 정책 에스컬레이션 경로가 있음

연결된 보안 주체는 IAM 정책을 직접 수정하여 추가 권한을 부여하고 중간 리소스 없이 자체 권한을 에스컬레이션할 수 있습니다.

신뢰 정책 하이재크 경로가 있음

연결된 보안 주체는 IAM 역할의 신뢰 정책을 수정하여가 해당 역할을 수임하여 역할의 권한을 얻도록 허용할 수 있습니다.

데이터 랜섬웨어 경로가 있음

연결된 보안 주체는 고객 관리형 AWS KMS 키로 Amazon S3 객체를 암호화한 다음 키 정책을 수정하는 등 랜섬웨어에 사용할 수 있는 방식으로 데이터를 암호화하거나 삭제할 수 있습니다.

제한 경로 제거

연결된 보안 주체는 권한 경계, 서비스 제어 정책 또는 리소스 기반 정책 거부 문과 같은 보안 제한을 제거하여 다른 보안 주체 또는 리소스 자체가 수행할 수 있는 작업을 확장할 수 있습니다.

패스 역할 생성 실행기 경로가 있음

연결된 보안 주체는 새 컴퓨팅 리소스(예: Lambda 함수 또는 Amazon EC2 인스턴스)를 생성하고 권한 있는 역할을 전달하여 새 리소스를 통해 자체 권한을 효과적으로 로세싱할 수 있습니다.

스왑 역할 기존 실행기 경로가 있음

연결된 보안 주체는 기존 컴퓨팅 리소스에 연결된 IAM 역할을 변경하여 더 권한이 있는 역할로 대체하여 액세스를 에스컬레이션할 수 있습니다.

역할 체인 에스컬레이션 경로가 있음

연결된 보안 주체는 일련의 역할을 수임할 수 있습니다. 여기서 체인의 각 역할은 점진적으로 더 광범위한 권한을 가지므로 궁극적으로 권한이 높은 역할에 도달합니다.

코드 삽입 권한이 있는 실행기 경로가 있음

연결된 보안 주체는 권한이 승격된 실행 중인 컴퓨팅 리소스에 코드를 주입하여 해당 리소스의 권한 있는 역할에 따라 임의 작업을 실행할 수 있습니다.

감사 추적 경로 비활성화

연결된 보안 주체는 CloudTrail과 같은 로깅 또는 모니터링 서비스를 비활성화하여 에스컬레이션 중 또는 에스컬레이션 후에 트랙을 효과적으로 처리할 수 있습니다.

기존 실행기 경로에 액세스할 수 있음

연결된 보안 주체는 기존 컴퓨팅 리소스를 호출하거나 연결하고 연결된 역할을 사용하여 권한 있는 작업을 수행할 수 있습니다.

자격 증명 마이닝 경로가 있음

연결된 보안 주체는 다른 보안 주체에 대한 새 장기 자격 증명(예: 액세스 키 또는 로그인 프로필)을 생성하여 암호 교체 또는 세션 만료 후에도 지속되는 영구 액세스 경로를 설정할 수 있습니다.

전달 역할 데이터 액세스 경로가 있음

연결된 보안 주체는 서비스 리소스를 생성하고 민감한 데이터에 액세스할 수 있는 역할을 전달하여 새 리소스를 통해 해당 데이터에 간접적으로 액세스할 수 있습니다.

역할 전달 작업 하이잭 경로가 있음

연결된 보안 주체는 예약된 작업 또는 이벤트 기반 작업(예: 이벤트에 의해 트리거된 Lambda 함수)에 역할을 전달하여 해당 역할의 권한으로 임의 코드를 실행할 수 있습니다.

단일 홉 데이터 액세스 경로가 있음

연결된 보안 주체는 중간 에스컬레이션 단계 없이 기존 권한을 통해 민감한 데이터 리소스(예: Amazon S3 버킷 또는 DynamoDB 테이블)에 직접 액세스할 수 있습니다.

기능 발전 경로가 있음

연결된 보안 주체에는 직접 할당된 권한 이상으로 전체 기능을 발전시키는 권한 에스컬레이션 경로가 있습니다. 이는 보다 구체적인 패턴과 일치하지 않는 경로에 대한 일반적인 분류입니다.

## Amazon EKS 클러스터에 대한 노출 문제 해결

AWS Security Hub는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터에 대한 노출 조사 결과를 생성할 수 있습니다.

노출 조사 결과와 관련된 Amazon EKS 클러스터 및 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 이러한 리소스 세부 정보는 Security Hub 콘솔에서 검색하거나 Security Hub CSPM API의 GetFindingsV2 작업을 통해 프로그래밍 방식으로 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침에 따라 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Amazon EKS 클러스터의 잘못된 구성 특성
  - Amazon EKS 클러스터가 퍼블릭 액세스를 허용
  - Amazon EKS 클러스터가 지원되지 않는 Kubernetes 버전을 사용
  - Amazon EKS 클러스터가 암호화되지 않은 Kubernetes 시크릿을 사용

- Amazon EKS 클러스터의 취약성 특성
  - Amazon EKS 클러스터에 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있는 컨테이너가 있음
  - Amazon EKS 클러스터에 소프트웨어 취약성이 있는 컨테이너가 있음
  - Amazon EKS 클러스터에는 End-Of-Life 운영 체제가 있는 컨테이너가 있습니다.
  - Amazon EKS 클러스터에는 악성 소프트웨어 패키지가 있는 컨테이너가 있습니다.
  - Amazon EKS 클러스터에 악성 파일이 있음

### Amazon EKS 클러스터의 잘못된 구성 특성

다음은 Amazon EKS 클러스터의 잘못된 구성 특성 및 제안된 문제 해결 단계입니다.

#### Amazon EKS 클러스터가 퍼블릭 액세스를 허용

Amazon EKS 클러스터 엔드포인트는 클러스터의 Kubernetes API 서버와 통신하는 데 사용하는 엔드포인트입니다. 기본적으로 이 엔드포인트는 인터넷에 공개됩니다. 퍼블릭 엔드포인트는 공격 표면 영역과 Kubernetes API 서버에 대한 무단 액세스 위험을 증가시켜 공격자가 클러스터 리소스에 액세스하거나 수정하거나 민감한 데이터에 액세스할 수 있습니다. 보안 모범 사례에 따라 Amazon EKS 클러스터 엔드포인트에 대한 액세스를 필요한 IP 범위로만 제한합니다.

##### 문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

###### 엔드포인트 액세스 수정

노출 조사 결과에서 리소스를 엽니다. 그러면 영향을 받는 Amazon EKS 클러스터가 열립니다. 프라이빗 액세스, 퍼블릭 액세스 또는 둘 다를 사용하도록 클러스터를 구성할 수 있습니다.

프라이빗 액세스를 사용하면 클러스터의 VPC 내에서 비롯된 Kubernetes API 요청이 프라이빗 VPC 엔드포인트를 사용합니다. 퍼블릭 액세스를 사용하면 클러스터의 VPC 외부에서 시작된 Kubernetes API 요청이 퍼블릭 엔드포인트를 사용합니다.

###### 클러스터에 대한 퍼블릭 액세스 수정 또는 제거

기존 클러스터의 엔드포인트 액세스를 수정하려면 Amazon Elastic Kubernetes Service 사용 설명서의 클러스터 엔드포인트 액세스 수정을 참조하세요. 특정 IP 범위 또는 보안 그룹을 기반으로 보다 제한적인 규칙을 구현합니다. 제한된 퍼블릭 액세스가 필요한 경우 액세스를 특정 CIDR 블록 범위로 제한하거나 접두사 목록을 사용합니다.

Amazon EKS 클러스터가 지원되지 않는 Kubernetes 버전을 사용

Amazon EKS는 각 Kubernetes 버전을 제한된 기간 동안 지원합니다. 오래된 버전에 대해서는 CVE 패치가 릴리스되지 않으므로, 지원되지 않는 Kubernetes 버전으로 클러스터를 실행하면 환경이 보안 취약성에 노출될 수 있습니다. 지원되지 않는 버전에는 공격자가 악용할 수 있는 알려진 보안 취약성이 포함될 수 있고 최신 버전에서 사용할 수 있는 보안 기능이 없을 수 있습니다. 보안 모범 사례에 따라 Kubernetes 버전을 최신 상태로 유지합니다.

문제 해결: Kubernetes 버전 업데이트

노출 조사 결과에서 리소스를 엽니다. 그러면 영향을 받는 Amazon EKS 클러스터가 열립니다. 클러스터를 업데이트하기 전에 Amazon Elastic Kubernetes Service 사용 설명서의 표준 지원으로 사용 가능한 버전에서 현재 지원되는 Kubernetes 버전 목록을 검토하세요.

Amazon EKS 클러스터가 암호화되지 않은 Kubernetes 시크릿을 사용

기본적으로 Kubernetes 시크릿은 API 서버의 기본 데이터 저장소(etcd)에 암호화되지 않은 상태로 저장됩니다. API 액세스 또는 etcd에 대한 액세스 권한이 있는 모든 사용자는 시크릿을 검색하거나 수정할 수 있습니다. 이를 방지하려면 Kubernetes 시크릿을 저장 시 암호화해야 합니다. Kubernetes 시크릿이 암호화되지 않은 경우 etcd가 손상되면 무단 액세스에 취약합니다. 시크릿에는 암호, API 토큰과 같은 민감한 정보가 포함되어 있는 경우가 많기 때문에 노출되면 다른 애플리케이션 및 데이터에 대한 무단 액세스로 이어질 수 있습니다. 보안 모범 사례에 따라 Kubernetes 보안 암호에 저장된 모든 민감한 정보를 암호화합니다.

문제 해결: Kubernetes 보안 암호 암호화

Amazon EKS는 봉투 암호화를 통해 KMS 키를 사용하는 Kubernetes 시크릿 암호화를 지원합니다. EKS 클러스터에 대해 Kubernetes 시크릿 암호화를 활성화하려면 Amazon EKS 사용 설명서의 기존 클러스터에서 KMS를 사용하여 Kubernetes 시크릿 암호화를 참조하세요.

Amazon EKS 클러스터의 취약성 특성

다음은 Amazon EKS 클러스터의 취약성 특성입니다.

Amazon EKS 클러스터에 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있는 컨테이너가 있음

Amazon EKS 클러스터에 설치된 소프트웨어 패키지는 일반 취약성 및 노출(CVE)에 노출될 수 있습니다. 중요 CVEs AWS 환경에 심각한 보안 위험을 초래합니다. 권한이 없는 사용자는 이러한 패치되지 않은 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스

할 수 있습니다. 악용 가능성이 높은 심각한 취약성은 악용 코드가 이미 공개되어 있고 공격자 또는 자동 스캔 도구가 이를 적극적으로 사용할 수 있으므로 즉각적인 보안 위협을 나타냅니다. 보안 모범 사례에 따라 이러한 취약성을 패치하여 공격으로부터 인스턴스를 보호합니다.

문제 해결: 영향을 받는 인스턴스 업데이트

컨테이너 이미지를 식별된 취약성에 대한 보안 수정 사항이 포함된 최신 버전으로 업데이트합니다. 여기에는 일반적으로 업데이트된 기본 이미지 또는 종속성을 사용하여 컨테이너 이미지를 재구축한 다음 새 이미지를 Amazon EKS 클러스터에 배포하는 작업이 포함됩니다.

Amazon EKS 클러스터에 소프트웨어 취약성이 있는 컨테이너가 있음

Amazon EKS 클러스터에 설치된 소프트웨어 패키지는 일반 취약성 및 노출(CVE)에 노출될 수 있습니다. 비중요 CVE는 중요 CVE에 비해 심각도 또는 악용 가능성이 낮은 보안 약점을 나타냅니다. 이러한 취약성은 즉각적인 위험을 초래하지 않지만 공격자는 패치되지 않은 이러한 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습니다. 보안 모범 사례에 따라 이러한 취약성을 패치하여 공격으로부터 인스턴스를 보호합니다.

문제 해결: 영향을 받는 인스턴스 업데이트

컨테이너 이미지를 식별된 취약성에 대한 보안 수정 사항이 포함된 최신 버전으로 업데이트합니다. 여기에는 일반적으로 업데이트된 기본 이미지 또는 종속성을 사용하여 컨테이너 이미지를 재구축한 다음 새 이미지를 Amazon EKS 클러스터에 배포하는 작업이 포함됩니다.

Amazon EKS 클러스터에는 End-Of-Life 운영 체제가 있는 컨테이너가 있습니다.

Amazon EKS 컨테이너 이미지는 원래 개발자가 더 이상 지원하지 않거나 유지 관리하지 않는 end-of-life 운영 체제를 사용합니다. 이렇게 하면 컨테이너가 보안 취약성 및 잠재적 공격에 노출됩니다. 운영 체제end-of-life하면 공급업체는 일반적으로 새로운 보안 권고 릴리스를 중단합니다. 공급업체 피드에서 기존 보안 권고를 제거할 수도 있습니다. 따라서 Amazon InspectorCVEs에 대한 결과 생성을 잠재적으로 중지하여 보안 적용 범위에 추가 격차를 초래할 수 있습니다.

Amazon Inspector에서 감지할 수 있는 수명이 다한 운영 체제에 대한 자세한 내용은 Amazon Inspector 사용 설명서의 중단된 운영 체제를 참조하세요. Amazon Inspector

문제 해결: 지원되는 운영 체제 버전으로 업데이트

지원되는 운영 체제 버전으로 업데이트합니다. 노출 조사 결과에서 리소스를 열어 영향을 받는 리소스에 액세스합니다. 컨테이너 이미지에서 운영 체제 버전을 업데이트하기 전에 현재 지원되는 OS 버전 목록은 Amazon Inspector 사용 설명서의 지원되는 운영 체제에서 사용 가능한 버전을 검토하세요.

Amazon Inspector 컨테이너 이미지를 업데이트한 후 컨테이너를 다시 빌드하고 Amazon EKS 클러스터에 다시 배포합니다.

Amazon EKS 클러스터에는 악성 소프트웨어 패키지가 있는 컨테이너가 있습니다.

악성 패키지는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함된 소프트웨어 구성 요소입니다. 공격자는 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있으므로 악의적인 패키지는 Amazon EKS 클러스터에 활발하고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 패키지를 제거하여 잠재적 공격으로부터 클러스터를 보호합니다.

문제 해결: 악성 패키지 제거

특성의 취약성 탭에 있는 참조 섹션에서 악성 패키지 세부 정보를 검토하여 위협을 이해합니다. 컨테이너 이미지에서 식별된 악성 패키지를 제거합니다. 그런 다음 손상된 이미지가 있는 포드를 삭제합니다.

업데이트된 컨테이너 이미지를 사용하도록 Kubernetes 배포를 업데이트합니다. 그런 다음 변경 사항을 배포하고 포드를 다시 배포합니다.

Amazon EKS 클러스터에 악성 파일이 있음

악성 파일에는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함되어 있습니다. 공격자는 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있으므로 악의적인 파일은 클러스터에 활발하고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 파일을 제거하여 잠재적 공격으로부터 클러스터를 보호합니다.

문제 해결: 악성 파일 제거

악성 파일이 있는 특정 Amazon Elastic Block Store(Amazon EBS) 볼륨을 식별하려면 특성의 결과 세부 정보의 리소스 섹션을 검토하세요. 악성 파일로 볼륨을 식별한 후 식별된 악성 파일을 제거합니다. 악성 파일을 제거한 후에는 스캔을 수행하여 악성 파일에 의해 설치되었을 수 있는 모든 파일이 제거되었는지 확인하는 것이 좋습니다. 자세한 내용은의 GuardDuty에서 온디맨드 맬웨어 스캔 시작을 참조하세요.

## IAM 사용자에 대한 노출 문제 해결

AWS Security Hub는 AWS Identity and Access Management (IAM) 사용자에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 IAM 사용자 및 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침은 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

IAM 모범 사례에서는 개별 IAM 사용자를 생성하는 대신 IAM 역할을 생성하거나 ID 제공업체와의 페더레이션을 사용하여 임시 자격 증명을 통해 AWS 에 액세스할 것을 권장합니다. 조직 및 사용 사례에 대한 옵션인 경우 IAM 사용자를 사용하는 대신 역할 또는 페더레이션으로 전환합니다. 자세한 내용은 IAM 사용자 설명서에서 IAM 사용자를 참조하세요.

목차


- IAM 사용자의 잘못된 구성 특성
  - IAM 사용자에게 MFA가 활성화되어 있지 않음
  - IAM 사용자의 AWS 계정에 약한 암호 정책이 있습니다.
  - IAM 사용자에게 교체되지 않은 액세스 키가 있음
  - IAM 사용자에게 KMS 키 복호화에 대한 무제한 액세스를 허용하는 정책이 있음
- IAM 사용자를 위한 미사용 액세스 특성
- IAM 사용자의 영향 특성
  - 전체 제어 권한 있는 실행기 경로 보유
  - 직접 정책 에스컬레이션 경로가 있음
  - 신뢰 정책 하이재크 경로가 있음
  - 데이터 랜섬웨어 경로가 있음
  - 제한 경로 제거
  - 패스 역할 생성 실행기 경로가 있음
  - 스왑 역할 기존 실행기 경로가 있음
  - 역할 체인 에스컬레이션 경로가 있음

- 코드 삽입 권한이 있는 실행기 경로가 있음
- 감사 추적 경로 비활성화
- 기존 실행기 경로에 액세스할 수 있음
- 자격 증명 마이닝 경로가 있음
- 전달 역할 데이터 액세스 경로가 있음
- 역할 전달 작업 하이재크 경로가 있음
- 단일 홉 데이터 액세스 경로가 있음
- 기능 발전 경로가 있음

IAM 사용자의 잘못된 구성 특성

다음은 IAM 사용자의 잘못된 구성 특성 및 제안된 문제 해결 단계입니다.

IAM 사용자에게 MFA가 활성화되어 있지 않음

다중 인증(MFA)을 통해 사용자 이름 및 비밀번호 외에 보호 계층이 한 단계 더 추가됩니다. MFA가 활성화되고 IAM 사용자가 AWS 웹 사이트에 로그인하면 AWS MFA 디바이스에서 사용자 이름, 암호 및 인증 코드를 입력하라는 메시지가 표시됩니다. 인증 보안 주체는 시간에 민감한 키를 내보내는 디바이스를 가지고 있어야 하며 보안 인증에 대한 지식이 있어야 합니다. MFA가 없으면 사용자의 암호가 손상되면 공격자는 사용자의 AWS 권한에 대한 전체 액세스 권한을 얻게 됩니다. 표준 보안 원칙에 따라 AWS Management Console 액세스 권한이 있는 모든 계정 및 사용자에 대해 MFA를 활성화합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

MFA 유형 검토

AWS 는 다음 MFA 유형을 지원합니다.

- 패스키 및 보안 키
- 가상 인증 애플리케이션
- 하드웨어 TOTP 토큰

물리적 디바이스를 사용한 인증은 일반적으로 더 엄격한 보안 보호를 제공하지만, 어떤 유형의 MFA를 사용해도 MFA를 비활성화하는 것보다 안전합니다.

MFA 활성화

요구 사항에 맞는 MFA 유형을 활성화하려면 IAM 사용자 설명서의 IAM의AWS 다중 인증을 참조하세요. 구현하려는 특정 MFA 유형에 대한 단계를 따릅니다. 많은 사용자를 관리하는 조직의 경우 민감한 리소스에 대한 액세스에 MFA를 요구해야 할 수 있습니다.

IAM 사용자의 AWS 계정에 약한 암호 정책이 있습니다.

암호 정책은 IAM 사용자 암호에 대한 최소 복잡성 요구 사항을 적용하여 무단 액세스로부터 보호하는 데 도움이 됩니다. 강력한 암호 정책이 없으면 암호 추측 또는 무차별 대입 공격을 통해 사용자 계정이 손상될 위험이 증가합니다. 표준 보안 원칙에 따라 강력한 암호 정책을 구현하여 사용자가 추측하기 어려운 복잡한 암호를 생성할 수 있도록 합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

강력한 암호 정책 구성

IAM 대시보드로 이동하여 계정 설정으로 이동합니다. 최소 길이, 필요한 문자 유형, 암호 만료 설정 등 계정의 현재 암호 정책 설정을 검토합니다.

암호 정책을 설정할 때는 최소한 다음 모범 사례를 따르십시오.

- 대문자가 한 개 이상이어야 합니다.
- 소문자가 한 개 이상이어야 합니다.
- 기호가 한 개 이상이어야 합니다.
- 숫자가 한 개 이상이어야 합니다.
- 최소 8자 이상이어야 합니다.

추가 보안 고려 사항

강력한 암호 정책 외에도 다음과 같은 추가 보안 조치를 고려하세요.

- MFA는 추가 형식의 인증을 요구하여 보안 계층을 추가합니다. 그러면 자격 증명이 침해되더라도 무단 액세스를 방지할 수 있습니다.
- 조건 요소를 설정하여 소스 IP 또는 MFA 수명과 같은 요인에 따라 관리 권한을 사용할 수 있는 시기 및 방법을 제한합니다.

IAM 사용자에게 교체되지 않은 액세스 키가 있음

액세스 키는 AWS 리소스에 프로그래밍 방식으로 액세스할 수 있는 액세스 키 ID와 보안 액세스 키로 구성됩니다. 액세스 키가 장기간 변경되지 않으면 손상된 경우 무단 액세스 위험이 증가합니다. 보안 모범 사례에 따라 90일마다 액세스 키를 교체하여 공격자가 손상된 자격 증명을 사용할 기회를 최소화합니다.

문제 해결: 액세스 키 교체

노출 조사 결과에서 리소스를 엽니다. 그러면 사용자 세부 정보 창이 열립니다. 액세스 키를 교체하려면 IAM 사용자 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요.

IAM 사용자에게 KMS 키 복호화에 대한 무제한 액세스를 허용하는 정책이 있음

AWS KMS 를 사용하면 데이터를 보호하는 데 사용되는 암호화 키를 생성하고 관리할 수 있습니다. 모든 KMS 키에 대해 무제한 AWS KMS 복호화 권한(예: `kms:Decrypt` 또는 `kms:ReEncryptFrom`)을 허용하는 IAM 정책은 IAM 사용자의 자격 증명이 손상되면 무단 데이터 액세스로 이어질 수 있습니다. 공격자가 이러한 자격 증명에 액세스할 경우 사용자 환경에서 암호화된 데이터를 해독할 수 있으며, 여기에는 민감한 데이터가 포함될 수 있습니다. 보안 모범 사례에 따라 AWS KMS 복호화 권한을 사용자에게 직무에 필요한 특정 키로만 제한하여 최소 권한을 구현합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

최소 권한 액세스 구현

노출 조사 결과에서 리소스를 엽니다. 그러면 IAM 정책 창이 열립니다. KMS에서 kms:Decrypt 또는 `kms:ReEncryptFrom` 또는 `KMS:*`를 허용하고 리소스 사양이 `"*"`인 권한을 찾습니다.

AWS KMS 복호화 권한을 필요한 특정 키로만 제한하도록 정책을 업데이트합니다. 정책을 수정하여 `"*"` 리소스를 필수 AWS KMS 키의 특정 ARNs.

보안 구성 고려 사항

이러한 권한을 사용할 수 있는 시기를 추가로 제한하는 조건을 추가하는 것이 좋습니다. 예를 들어 복호화 작업을 특정 VPC 엔드포인트 또는 소스 IP 범위로 제한할 수 있습니다. 특정 KMS 키를 사용할 수 있는 사용자를 추가로 제한하도록 키 정책을 구성할 수도 있습니다.

IAM 사용자를 위한 미사용 액세스 특성

IAM 사용자에게 미사용 권한, 액세스 키 또는 암호가 있는 경우 Security Hub는 해당 사용자의 노출 조사 결과에 이를 컨텍스트 특성으로 포함할 수 있습니다. 이러한 특성은 서비스 관리형 IAM Access

Analyzer에서 생성되며 사용자의 보안 태세에 대한 추가 컨텍스트를 제공합니다. 미사용 액세스 특성은 노출 결과의 주요 원인이 아니지만 사용자에게 필요 이상의 권한이 있음을 나타내므로 사용자의 자격 증명이 손상되면 잠재적 영향이 커집니다.

특히 미사용 권한의 경우 범위가 축소된 대체 정책을 보여주는 최소 권한 정책 권장 사항을 생성할 수 있습니다. 자세한 내용은 the section called “정책 권장 사항” 단원을 참조하십시오.

IAM 사용자의 영향 특성

영향 특성은 노출의 잠재적 폭발 반경을 설명합니다. Security Hub는 IAM 사용자와 연결된 AWS Identity and Access Management 보안 주체의 유효 권한을 분석하여 IAM 사용자가 손상된 경우 공격자가 도달할 수 있는 다운스트림 리소스를 결정합니다. 각 영향 특성은 특정 권한 에스컬레이션 패턴을 식별합니다. 블래스트 반경을 줄이려면 각 특성에 설명된 권한 경로를 검토하고 불필요한 권한을 제거합니다.

표준 보안 원칙에 따라 작업을 수행하는 데 필요한 권한만 제공하여 최소 권한을 부여합니다. 광범위한 정책을 필요한 특정 작업 및 리소스만 부여하는 범위 축소 정책으로 바꿉니다. 제거할 미사용 권한을 식별하려면 IAM Access Analyzer를 사용하여 액세스 기록을 기반으로 권장 사항을 생성합니다. 자세한 내용은 IAM 사용 설명서의 외부 및 미사용 액세스 결과 및 최소 권한 적용을 참조하세요.

전체 제어 권한 있는 실행기 경로 보유

연결된 보안 주체는 이미 승격된 권한이 있는 컴퓨팅 리소스에 역할을 전달하고 코드를 주입할 수 있습니다. 이를 통해 보안 주체는 실행기를 완전히 제어하고 실행기의 역할이 허용하는 모든 작업을 수행할 수 있습니다.

직접 정책 에스컬레이션 경로가 있음

연결된 보안 주체는 IAM 정책을 직접 수정하여 추가 권한을 부여하고 중간 리소스 없이 자체 권한을 에스컬레이션할 수 있습니다.

신뢰 정책 하이재크 경로가 있음

연결된 보안 주체는 IAM 역할의 신뢰 정책을 수정하여가 해당 역할을 수임하여 역할의 권한을 얻도록 허용할 수 있습니다.

데이터 랜섬웨어 경로가 있음

연결된 보안 주체는 고객 관리형 AWS KMS 키로 Amazon S3 객체를 암호화한 다음 키 정책을 수정하는 등 랜섬웨어에 사용할 수 있는 방식으로 데이터를 암호화하거나 삭제할 수 있습니다.

제한 경로 제거

연결된 보안 주체는 권한 경계, 서비스 제어 정책 또는 리소스 기반 정책 거부 문과 같은 보안 제한을 제거하여 다른 보안 주체 또는 리소스 자체가 수행할 수 있는 작업을 확장할 수 있습니다.

패스 역할 생성 실행기 경로가 있음

연결된 보안 주체는 새 컴퓨팅 리소스(예: Lambda 함수 또는 Amazon EC2 인스턴스)를 생성하고 권한 있는 역할을 전달하여 새 리소스를 통해 자체 권한을 효과적으로 로세싱할 수 있습니다.

스왑 역할 기존 실행기 경로가 있음

연결된 보안 주체는 기존 컴퓨팅 리소스에 연결된 IAM 역할을 변경하여 더 권한이 있는 역할로 대체하여 액세스를 에스컬레이션할 수 있습니다.

역할 체인 에스컬레이션 경로가 있음

연결된 보안 주체는 일련의 역할을 수임할 수 있습니다. 여기서 체인의 각 역할은 점진적으로 더 광범위한 권한을 가지므로 궁극적으로 권한이 높은 역할에 도달합니다.

코드 삽입 권한이 있는 실행기 경로가 있음

연결된 보안 주체는 권한이 승격된 실행 중인 컴퓨팅 리소스에 코드를 주입하여 해당 리소스의 권한 있는 역할에 따라 임의 작업을 실행할 수 있습니다.

감사 추적 경로 비활성화

연결된 보안 주체는 CloudTrail과 같은 로깅 또는 모니터링 서비스를 비활성화하여 에스컬레이션 중 또는 에스컬레이션 후에 트랙을 효과적으로 처리할 수 있습니다.

기존 실행기 경로에 액세스할 수 있음

연결된 보안 주체는 기존 컴퓨팅 리소스를 호출하거나 연결하고 연결된 역할을 사용하여 권한 있는 작업을 수행할 수 있습니다.

자격 증명 마이닝 경로가 있음

연결된 보안 주체는 다른 보안 주체에 대한 새 장기 자격 증명(예: 액세스 키 또는 로그인 프로필)을 생성하여 암호 교체 또는 세션 만료 후에도 지속되는 영구 액세스 경로를 설정할 수 있습니다.

전달 역할 데이터 액세스 경로가 있음

연결된 보안 주체는 서비스 리소스를 생성하고 민감한 데이터에 액세스할 수 있는 역할을 전달하여 새 리소스를 통해 해당 데이터에 간접적으로 액세스할 수 있습니다.

역할 전달 작업 하이재크 경로가 있음

연결된 보안 주체는 예약된 작업 또는 이벤트 기반 작업(예: 이벤트에 의해 트리거된 Lambda 함수)에 역할을 전달하여 해당 역할의 권한으로 임의 코드를 실행할 수 있습니다.

단일 홉 데이터 액세스 경로가 있음

연결된 보안 주체는 중간 에스컬레이션 단계 없이 기존 권한을 통해 민감한 데이터 리소스(예: Amazon S3 버킷 또는 DynamoDB 테이블)에 직접 액세스할 수 있습니다.

기능 발전 경로가 있음

연결된 보안 주체에는 직접 할당된 권한 이상으로 전체 기능을 발전시키는 권한 에스컬레이션 경로가 있습니다. 이는 보다 구체적인 패턴과 일치하지 않는 경로에 대한 일반적인 분류입니다.

## AWS Lambda 함수에 대한 노출 문제 해결

AWS Security Hub는 AWS Lambda 함수에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Lambda 함수 및 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침은 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Lambda 함수의 잘못된 구성 특성
  - Lambda 함수가 Amazon VPC 외부에 배포됨
  - Lambda 함수는 권한 부여 없이 API Gateway를 통해 액세스할 수 있습니다.

- Lambda 함수의 연결성 특성
  - Lambda 함수는 공개적으로 간접적으로 호출될 수 있습니다
- Lambda 함수의 취약성 특성
  - Lambda 함수에 네트워크 탐색 가능 소프트웨어 취약성이 있음
  - Lambda 함수에 소프트웨어 취약성이 있음
  - Lambda 함수에 악성 소프트웨어 패키지가 있음
  - Lambda 함수에 코드 취약성이 있음
- Lambda 함수의 영향 특성
  - 전체 제어 권한 있는 실행기 경로 보유
  - 직접 정책 에스컬레이션 경로가 있음
  - 신뢰 정책 하이재크 경로가 있음
  - 데이터 랜섬웨어 경로가 있음
  - 제한 경로 제거
  - 패스 역할 생성 실행기 경로가 있음
  - 스왑 역할 기존 실행기 경로가 있음
  - 역할 체인 에스컬레이션 경로가 있음
  - 코드 삽입 권한이 있는 실행기 경로가 있음
  - 감사 추적 경로 비활성화
  - 기존 실행기 경로에 액세스할 수 있음
  - 자격 증명 마이닝 경로가 있음
  - 전달 역할 데이터 액세스 경로가 있음
  - 역할 전달 작업 하이잭 경로가 있음
  - 단일 홉 데이터 액세스 경로가 있음
  - 기능 발전 경로가 있음

### Lambda 함수의 잘못된 구성 특성

다음은 Lambda 함수의 잘못된 구성 특성 및 제안된 문제 해결 단계입니다.

#### Lambda 함수가 Amazon VPC 외부에 배포됨

Lambda 함수는 기본적으로 퍼블릭 인터넷에 액세스하도록 배포됩니다. 이 기본 구성은 Lambda 함수에 AWS 서비스 엔드포인트 및 외부 APIs에 연결할 수 있는 기능을 제공하지만 잠재적인 보안 위험에

도 노출됩니다. 인터넷에 액세스할 수 있는 기능은 손상된 경우 데이터를 유출하거나 승인되지 않은 서버와 통신하는 데 사용될 수 있고 외부 액터의 진입점이 될 수 있습니다. Amazon VPC는 Lambda 함수가 정의된 프라이빗 네트워크 내의 리소스와만 통신하도록 제한하여 네트워크 격리를 제공합니다. 표준 보안 원칙에 따라 VPC 내에 Lambda 함수를 배포하여 네트워크 격리를 통해 보안을 개선합니다.

문제 해결: VPC에 함수 연결

노출 결과에서 리소스 링크를 선택합니다. 그러면 Lambda 콘솔에서 Lambda 함수가 열립니다. 네트워크 액세스를 제한하여 Lambda 함수를 보호하려면 적절한 네트워크 제어가 설정된 VPC에 연결합니다.

함수를 VPC에 연결하기 전에 필요할 수 있는 모든 AWS 서비스 액세스를 계획합니다. NAT 게이트웨이 또는 VPC 엔드포인트가 없는 프라이빗 서브넷의 함수는 AWS 서비스 APIs에 도달할 수 없기 때문입니다. Lambda 함수를 계정의 Amazon VPC에 연결하는 방법에 대한 자세한 내용은 Lambda 함수를 AWS 계정의 Amazon VPC에 연결을 참조하세요. 함수가 프라이빗 서브넷 내에서 서비스에 액세스해야 하는 경우 인터넷 액세스 없이 AWS 서비스 연결에 VPC 엔드포인트를 사용하는 것이 좋습니다. 프라이빗 서브넷에서 아웃바운드 인터넷 연결이 필요한 경우 NAT 게이트웨이를 구성합니다.

Lambda 함수는 권한 부여 없이 API Gateway를 통해 액세스할 수 있습니다.

권한이 없는 API Gateway 메서드를 사용하면 API Gateway에 액세스할 수 있는 모든 호출자가 자격 증명 확인 없이 통합 Lambda 함수를 호출할 수 있습니다. 호출자는 적절한 권한 부여 없이 Lambda 함수를 호출하여 잠재적으로 함수 기능, 리소스 소비, 민감한 데이터에 대한 액세스 또는 무단 작업을 침해할 수 있으므로이 구성은 보안 위험을 초래합니다. API Gateway에는 네트워크 수준 액세스 제어가 있을 수 있지만 메서드 수준 권한 부여가 없으면 API Gateway에 대한 네트워크 액세스 권한이 있는 모든 호출자가 함수를 무료로 호출할 수 있습니다. 보안 모범 사례에 따라 Lambda 함수와 통합되는 API Gateway 메서드에 대한 적절한 권한 부여 메커니즘을 구현합니다.

문제 해결: API Gateway 인증 구성

노출의 리소스 탭에서 리소스 링크를 선택하여 API Gateway 메서드에 액세스합니다. 현재 권한 부여 구성을 검토하고 적절한 인증 메커니즘을 구현합니다.

API Gateway는 AWS IAM, Amazon Cognito 사용자 풀, Lambda 권한 부여자 및 API 키를 비롯한 여러 인증 옵션을 지원합니다. 보안 요구 사항 및 사용 사례에 가장 적합한 인증 방법을 선택합니다. 인증 구성에 대한 자세한 지침은 API Gateway 개발자 안내서의 API Gateway에서 REST API에 대한 액세스 제어 및 관리를 참조하세요.

Lambda 함수의 연결성 특성

다음은 Lambda 함수의 연결성 특성 및 제안된 문제 해결 단계입니다.

Lambda 함수는 공개적으로 간접적으로 호출될 수 있습니다

Lambda 리소스 기반 정책에 따라 함수를 간접적으로 호출할 수 있는 사용자가 결정됩니다. "*"를 보안 주체로 포함하는(또는 보안 주체가 전혀 없는) 리소스 정책이 있는 함수는 인증된 AWS 사용자가 호출할 수 있도록 허용합니다. 그러면 특히 민감한 데이터를 처리하거나 리소스를 수정하거나 권한이 상승된 함수에 상당한 위험이 발생합니다. 권한이 없는 사용자가 이 구성을 악용해 원치 않는 작업을 수행하여 잠재적으로 데이터를 노출하거나 리소스를 조작하거나 함수 기능을 남용할 수 있습니다. 보안 모범 사례에 따라 Lambda 함수 액세스를 승인된 보안 주체로만 제한합니다.

문제 해결: 함수의 리소스 기반 정책 수정

노출의 리소스 탭에서 하이퍼링크를 사용하여 리소스를 엽니다. 그러면 Lambda 콘솔에서 Lambda 함수가 열립니다. 리소스 기반 정책에서 승인된 AWS 계정 IDs 또는 특정 IAM 보안 주체(사용자, 역할 또는 서비스)만 지정하여 Lambda 함수에 대한 액세스를 제한합니다. 리소스 기반 정책은 프로그래밍 방식으로만 수정할 수 있습니다.

Lambda 함수의 취약성 특성

다음은 Lambda 함수의 취약성 특성 및 제안된 문제 해결 단계입니다.

Lambda 함수에 네트워크 탐색 가능 소프트웨어 취약성이 있음

Lambda 함수 코드에 사용되는 소프트웨어 패키지에는 악용 가능성이 높은 일반 취약성 및 노출(CVE)이 포함될 수 있습니다. 중요 CVEs AWS 환경에 심각한 보안 위험을 초래합니다. 공격자는 이러한 패치되지 않은 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습니다. 악용 가능성이 높은 심각한 취약성은 악용 코드가 이미 공개되어 있고 공격자 또는 자동 스캔 도구가 이를 적극적으로 사용할 수 있으므로 즉각적인 보안 위협을 나타냅니다. 보안 모범 사례에 따라 이러한 취약성을 패치하여 공격으로부터 함수를 보호합니다.

문제 해결: 영향을 받는 함수 업데이트

특성의 취약성 탭에서 참조 섹션을 검토합니다. 공급업체 설명서에는 특정 수정 지침이 포함될 수 있습니다. 공급업체 권장 절차에 따라 취약한 라이브러리를 최신 보안 버전으로 업데이트합니다.

일반적으로 문제 해결 워크플로는 Lambda 패키지를 zip 파일을 업로드하여 배포했는지 또는 컨테이너 이미지로 Lambda 함수를 생성하여 배포했는지에 따라 달라집니다. 라이브러리를 업데이트한 후 수정된 버전을 사용하도록 Lambda 함수 코드를 업데이트합니다. 그런 다음 업데이트된 버전을 배포합니다.

Lambda 함수에 소프트웨어 취약성이 있음

Lambda 함수는 중요 CVE에 비해 심각도 또는 악용 가능성이 낮은 보안 취약성을 포함할 수 있는 서드 파티 라이브러리 및 종속성을 사용하는 경우가 많습니다. 이러한 중요하지 않은 취약성은 즉시 악용 가능하지 않을 수는 있지만 여전히 다른 취약성과 함께 연결되어 함수를 손상시킬 수 있는 보안 약점을 나타냅니다. 시간이 지나면 이러한 취약성의 위험을 높이는 새로운 악용 기법도 등장할 수 있습니다. 표준 보안 원칙에 따라 이러한 취약성을 패치하여 안전한 환경을 유지합니다.

문제 해결: 영향을 받는 함수 업데이트

특성의 취약성 탭에서 참조 섹션을 검토합니다. 공급업체 설명서에는 특정 수정 지침이 포함될 수 있습니다. 공급업체 권장 절차에 따라 취약한 라이브러리를 최신 보안 버전으로 업데이트합니다.

일반적으로 문제 해결 워크플로는 Lambda 패키지를 zip 파일을 업로드하여 배포했는지 또는 컨테이너 이미지로 Lambda 함수를 생성하여 배포했는지에 따라 달라집니다. 라이브러리를 업데이트한 후 수정된 버전을 사용하도록 Lambda 함수 코드를 업데이트합니다. 그런 다음 업데이트된 버전을 배포합니다.

Lambda 함수에 악성 소프트웨어 패키지가 있음

악성 패키지는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함된 소프트웨어 구성 요소입니다. 공격자가 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있으므로 악성 패키지는 Lambda 함수에 능동적이고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 패키지를 제거하여 잠재적 공격으로부터 Lambda 함수를 보호합니다.

문제 해결: 악성 패키지 제거

특성의 취약성 탭에 있는 참조 섹션에서 악성 패키지 세부 정보를 검토하여 위협을 이해합니다. 함수 코드 및 종속성에서 식별된 악성 패키지를 제거합니다. 계층을 사용하는 함수의 경우 악성 패키지가 계층에 설치되어 있는지 확인하고 제거합니다.

배포 패키지 또는 컨테이너 이미지를 업데이트하여 악성 패키지를 제외한 다음 업데이트된 버전을 배포합니다. 지침은 .zip 파일 아카이브에 대한 .zip 파일 아카이브로 Lambda 함수 배포 또는 컨테이너 이미지에 대한 컨테이너 이미지를 사용하여 Lambda 함수 생성을 참조하세요.

Lambda 함수에 코드 취약성이 있음

Lambda 함수 애플리케이션 코드에는 위협 행위자가 악용할 수 있는 보안 취약성이 포함되어 있습니다. 코드 취약성에는 데이터 유출, 주입 결함, 누락된 암호화, 자동 코드 분석을 통해 식별되는 약한 암호화가 포함됩니다. 공격자는 이러한 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상

시키거나 다른 시스템에 액세스할 수 있으므로 이러한 취약성은 AWS 환경에 보안 위험을 초래할 수 있습니다. 코드 취약성은 다른 공격 벡터와 함께 연결되어 함수를 손상시킬 수 있는 보안 약점을 나타냅니다. 보안 모범 사례에 따라 이러한 코드 취약성을 해결하여 공격으로부터 함수를 보호합니다.

문제 해결: 영향을 받는 함수 업데이트

특성의 취약성 탭에서 참조 섹션을 검토합니다. Amazon Inspector 조사 결과에는 취약한 코드 위치를 보여주는 특정 수정 지침 및 코드 조각이 포함될 수 있습니다. 제공된 plug-and-play 코드 블록을 사용하거나 보안 코딩 관행을 구현하여 함수 코드에서 식별된 보안 문제를 해결합니다.

코드가 의도한 대로 작동하는지 확인하기 위해 코드 수정 제안을 편집해야 할 수 있으므로 채택하기 전에 항상 검토하세요. 취약성을 수정한 후 수정된 버전을 사용하도록 Lambda 함수 코드를 업데이트합니다. 지침은 AWS Lambda 개발자 안내서의 함수 코드 업데이트를 참조하세요.

그런 다음 업데이트된 버전을 배포합니다. 지침은 .zip 파일 아카이브에 대한 .zip 파일 아카이브로 Lambda 함수 배포 또는 컨테이너 이미지에 대한 컨테이너 이미지를 사용하여 Lambda 함수 생성을 참조하세요. Amazon Inspector 코드 스캔에 대한 자세한 내용은 Amazon Inspector 사용 설명서의 Amazon Inspector Lambda 코드 스캔을 참조하세요. Amazon Inspector

Lambda 함수의 영향 특성

영향 특성은 노출의 잠재적 폭발 반경을 설명합니다. Security Hub는 Lambda 함수와 연결된 AWS Identity and Access Management 보안 주체의 유효 권한을 분석하여 함수가 손상된 경우 공격자가 도달할 수 있는 다운스트림 리소스를 결정합니다. 각 영향 특성은 특정 권한 에스컬레이션 패턴을 식별합니다. 블래스트 반경을 줄이려면 각 특성에 설명된 권한 경로를 검토하고 불필요한 권한을 제거합니다.

표준 보안 원칙에 따라 작업을 수행하는 데 필요한 권한만 제공하여 최소 권한을 부여합니다. 광범위한 정책을 필요한 특정 작업 및 리소스만 부여하는 범위 축소 정책으로 바꿉니다. 제거할 미사용 권한을 식별하려면 IAM Access Analyzer를 사용하여 액세스 기록을 기반으로 권장 사항을 생성합니다. 자세한 내용은 IAM 사용 설명서의 외부 및 미사용 액세스 결과 및 최소 권한 적용을 참조하세요.

전체 제어 권한 있는 실행기 경로 보유

연결된 보안 주체는 이미 승격된 권한이 있는 컴퓨팅 리소스에 역할을 전달하고 코드를 주입할 수 있습니다. 이를 통해 보안 주체는 실행기를 완전히 제어하고 실행기의 역할이 허용하는 모든 작업을 수행할 수 있습니다.

직접 정책 에스컬레이션 경로가 있음

연결된 보안 주체는 IAM 정책을 직접 수정하여 추가 권한을 부여하고 중간 리소스 없이 자체 권한을 에스컬레이션할 수 있습니다.

신뢰 정책 하이재크 경로가 있음

연결된 보안 주체는 IAM 역할의 신뢰 정책을 수정하여가 해당 역할을 수임하여 역할의 권한을 얻도록 허용할 수 있습니다.

데이터 랜섬웨어 경로가 있음

연결된 보안 주체는 고객 관리형 AWS KMS 키로 Amazon S3 객체를 암호화한 다음 키 정책을 수정하는 등 랜섬웨어에 사용할 수 있는 방식으로 데이터를 암호화하거나 삭제할 수 있습니다.

제한 경로 제거

연결된 보안 주체는 권한 경계, 서비스 제어 정책 또는 리소스 기반 정책 거부 문과 같은 보안 제한을 제거하여 다른 보안 주체 또는 리소스 자체가 수행할 수 있는 작업을 확장할 수 있습니다.

패스 역할 생성 실행기 경로가 있음

연결된 보안 주체는 새 컴퓨팅 리소스(예: Lambda 함수 또는 Amazon EC2 인스턴스)를 생성하고 권한 있는 역할을 전달하여 새 리소스를 통해 자체 권한을 효과적으로 로세싱할 수 있습니다.

스왑 역할 기존 실행기 경로가 있음

연결된 보안 주체는 기존 컴퓨팅 리소스에 연결된 IAM 역할을 변경하여 더 권한이 있는 역할로 대체하여 액세스를 에스컬레이션할 수 있습니다.

역할 체인 에스컬레이션 경로가 있음

연결된 보안 주체는 일련의 역할을 수임할 수 있습니다. 여기서 체인의 각 역할은 점진적으로 더 광범위한 권한을 가지므로 궁극적으로 권한이 높은 역할에 도달합니다.

코드 삽입 권한이 있는 실행기 경로가 있음

연결된 보안 주체는 권한이 승격된 실행 중인 컴퓨팅 리소스에 코드를 주입하여 해당 리소스의 권한 있는 역할에 따라 임의 작업을 실행할 수 있습니다.

감사 추적 경로 비활성화

연결된 보안 주체는 CloudTrail과 같은 로깅 또는 모니터링 서비스를 비활성화하여 에스컬레이션 중 또는 에스컬레이션 후에 트랙을 효과적으로 처리할 수 있습니다.

기존 실행기 경로에 액세스할 수 있음

연결된 보안 주체는 기존 컴퓨팅 리소스를 호출하거나 연결하고 연결된 역할을 사용하여 권한 있는 작업을 수행할 수 있습니다.

자격 증명 마이닝 경로가 있음

연결된 보안 주체는 다른 보안 주체에 대한 새 장기 자격 증명(예: 액세스 키 또는 로그인 프로필)을 생성하여 암호 교체 또는 세션 만료 후에도 지속되는 영구 액세스 경로를 설정할 수 있습니다.

전달 역할 데이터 액세스 경로가 있음

연결된 보안 주체는 서비스 리소스를 생성하고 민감한 데이터에 액세스할 수 있는 역할을 전달하여 새 리소스를 통해 해당 데이터에 간접적으로 액세스할 수 있습니다.

역할 전달 작업 하이잭 경로가 있음

연결된 보안 주체는 예약된 작업 또는 이벤트 기반 작업(예: 이벤트에 의해 트리거된 Lambda 함수)에 역할을 전달하여 해당 역할의 권한으로 임의 코드를 실행할 수 있습니다.

단일 홉 데이터 액세스 경로가 있음

연결된 보안 주체는 중간 에스컬레이션 단계 없이 기존 권한을 통해 민감한 데이터 리소스(예: Amazon S3 버킷 또는 DynamoDB 테이블)에 직접 액세스할 수 있습니다.

기능 발전 경로가 있음

연결된 보안 주체에는 직접 할당된 권한 이상으로 전체 기능을 발전시키는 권한 에스컬레이션 경로가 있습니다. 이는 보다 구체적인 패턴과 일치하지 않는 경로에 대한 일반적인 분류입니다.

## Amazon RDS 인스턴스 및 클러스터에 대한 노출 문제 해결

AWS Security Hub는 Amazon RDS 인스턴스 및 클러스터에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Amazon RDS 인스턴스 또는 클러스터와 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침에 따라 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Amazon RDS 인스턴스 및 클러스터의 구성 오류 특성
  - Amazon RDS DB 인스턴스가 퍼블릭 액세스로 구성됨
  - Amazon RDS DB 클러스터에 공개적으로 공유되는 스냅샷이 있음
  - Amazon RDS DB 인스턴스에 공개적으로 공유되는 스냅샷이 있음
  - Amazon RDS DB 인스턴스에 저장 시 암호화되지 않은 스냅샷이 있음
  - Amazon RDS DB 클러스터에 저장 시 암호화되지 않은 스냅샷이 있음
  - Amazon RDS DB 인스턴스에 개방형 보안 그룹이 있음
  - Amazon RDS DB 인스턴스에 IAM 데이터베이스 인증이 비활성화되어 있음
  - Amazon RDS DB 인스턴스가 기본 관리자 사용자 이름을 사용
  - Amazon RDS DB 클러스터가 기본 관리자 사용자 이름을 사용
  - Amazon RDS DB 인스턴스에 마이너 버전 자동 업그레이드가 비활성화되어 있음
  - Amazon RDS DB 인스턴스에 자동 백업이 비활성화되어 있음
  - Amazon RDS DB 인스턴스에 삭제 방지가 비활성화되어 있음
  - Amazon RDS DB 클러스터에 삭제 방지가 비활성화되어 있음
  - Amazon RDS DB 인스턴스가 데이터베이스 엔진에 기본 포트를 사용
  - Amazon RDS DB 인스턴스가 백업 계획에 포함되지 않음
- Amazon RDS DB 인스턴스의 민감한 데이터 특성
  - Amazon RDS DB 인스턴스에 민감한 데이터 포함


## Amazon RDS 인스턴스 및 클러스터의 구성 오류 특성

다음은 Amazon RDS 인스턴스 및 클러스터의 잘못된 구성 특성 및 수정 단계를 설명합니다.

### Amazon RDS DB 인스턴스가 퍼블릭 액세스로 구성됨

퍼블릭 액세스를 사용하는 Amazon RDS 인스턴스는 엔드포인트를 통해 인터넷에서 액세스할 수 있습니다. 퍼블릭 액세스가 인스턴스 기능에 필요한 경우도 있지만, 이러한 구성은 권한이 없는 사용자가

데이터베이스에 액세스하려고 시도하는 잠재적 공격 벡터로 사용할 수 있습니다. 공개적으로 액세스할 수 있는 데이터베이스는 포트 스캔, 무차별 대입 공격 및 악용 시도에 노출될 수 있습니다. 표준 보안 원칙에 따라 데이터베이스 리소스의 공개 노출을 제한합니다.

문제 해결: 퍼블릭 액세스 설정 수정

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 DB 인스턴스가 열립니다. 애플리케이션 아키텍처를 기반으로 DB 인스턴스에 퍼블릭 액세스가 필요한지 평가합니다. 자세한 내용은 Amazon RDS에서 퍼블릭 또는 프라이빗 액세스 설정을 참조하세요.

Amazon RDS DB 클러스터에 공개적으로 공유되는 스냅샷이 있음

퍼블릭 스냅샷은 권한이 없는 사용자에게 민감한 데이터를 노출할 AWS 계정가능성이 있는 모든 사용자가 액세스할 수 있습니다. AWS 계정 에는 이러한 퍼블릭 스냅샷을 복사하고이 스냅샷에서 DB 인스턴스를 생성할 수 있는 권한이 있으며, 이로 인해 데이터 침해 또는 무단 데이터 액세스가 발생할 수 있습니다. 보안 모범 사례에 따라 Amazon RDS 스냅샷에 대한 액세스를 신뢰할 수 있는 AWS 계정 및 조직으로만 제한합니다.

해결 방법: 프라이빗 액세스를 위한 Amazon RDS 스냅샷 구성

노출 조사 결과에서 하이퍼링크를 사용하여 리소스를 엽니다. 스냅샷 공유 설정을 수정하는 방법에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 스냅샷 공유를 참조하세요. 스냅샷 공유를 중지하는 방법에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 스냅샷 공유 중지를 참조하세요.

Amazon RDS DB 인스턴스에 공개적으로 공유되는 스냅샷이 있음

퍼블릭 스냅샷은 권한이 없는 사용자에게 민감한 데이터를 노출할 AWS 계정가능성이 있는 모든 사용자가 액세스할 수 있습니다. AWS 계정 에는 이러한 퍼블릭 스냅샷을 복사하고이 스냅샷에서 DB 인스턴스를 생성할 수 있는 권한이 있으며, 이로 인해 데이터 침해 또는 무단 데이터 액세스가 발생할 수 있습니다. 보안 모범 사례에 따라 Amazon RDS 스냅샷에 대한 액세스를 신뢰할 수 있는 AWS 계정 및 조직으로만 제한합니다.

해결 방법: 프라이빗 액세스를 위한 Amazon RDS 스냅샷 구성

노출 조사 결과에서 하이퍼링크를 사용하여 리소스를 엽니다. 스냅샷 공유 설정을 수정하는 방법에 대한 자세한 내용은 Amazon RDS 사용 설명서의 DB 스냅샷 공유를 참조하세요. 스냅샷 공유를 중지하는 방법에 대한 자세한 내용은 Amazon RDS 사용 설명서의 DB 스냅샷 공유 중지를 참조하세요.

Amazon RDS DB 인스턴스에 저장 시 암호화되지 않은 스냅샷이 있음

암호화되지 않은 Amazon RDS DB 인스턴스 스냅샷은 스토리지 계층에 대한 무단 액세스가 발생할 경우 민감한 데이터를 노출시킬 수 있습니다. 암호화가 없으면 무단 액세스를 통해 스냅샷의 데이터가 노

출될 수 있습니다. 이로 인해 데이터 위반 및 규정 준수 위반의 위험이 발생합니다. 보안 모범 사례에 따라 모든 데이터베이스 리소스와 백업을 암호화하여 데이터 기밀성을 유지합니다.

문제 해결: 영향을 받는 리소스 업데이트

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 스냅샷이 열립니다. 기존의 암호화되지 않은 스냅샷을 직접 암호화할 수는 없습니다.

대신, 암호화되지 않은 스냅샷의 암호화된 사본을 생성합니다. 자세한 지침은 Amazon Aurora 사용 설명서의 DB 클러스터 스냅샷 복사 및 Amazon RDS 리소스 암호화를 참조하세요.

Amazon RDS DB 클러스터에 저장 시 암호화되지 않은 스냅샷이 있음

암호화되지 않은 Amazon RDS DB 클러스터 스냅샷은 스토리지 계층에 대한 무단 액세스가 발생할 경우 민감한 데이터를 노출시킬 수 있습니다. 암호화가 없으면 무단 액세스를 통해 스냅샷의 데이터가 노출될 수 있습니다. 이로 인해 데이터 위반 및 규정 준수 위반의 위험이 발생합니다. 보안 모범 사례에 따라 모든 데이터베이스 리소스와 백업을 암호화하여 데이터 기밀성을 유지합니다.

문제 해결: 스냅샷의 암호화된 복사본 생성

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 스냅샷이 열립니다. 기존의 암호화되지 않은 스냅샷을 직접 암호화할 수는 없습니다.

대신, 암호화되지 않은 스냅샷의 암호화된 사본을 생성합니다. 자세한 지침은 Amazon Aurora 사용 설명서의 DB 클러스터 스냅샷 복사 및 Amazon RDS 리소스 암호화를 참조하세요.

Amazon RDS DB 인스턴스에 개방형 보안 그룹이 있음

보안 그룹은 Amazon RDS 인스턴스에 대한 인바운드 및 아웃바운드 트래픽을 제어하는 가상 방화벽 역할을 합니다. 모든 IP 주소로부터 무제한 액세스를 허용하는 개방형 보안 그룹은 데이터베이스 인스턴스를 무단 액세스 및 잠재적 공격에 노출시킬 수 있습니다. 표준 보안 원칙에 따라 보안 그룹 액세스를 특정 IP 주소 및 포트로 제한하여 최소 권한 원칙을 유지합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

보안 그룹 규칙 검토 및 현재 구성 평가

노출 조사 결과에서 DB 인스턴스 보안 그룹의 리소스를 엽니다. `(0.0.0.0/0 or ::/0)`과 같은 광범위한 IP 범위에서 액세스할 수 있는 개방 포트를 평가합니다. 보안 그룹 세부 정보를 보는 방법에 대한 자세한 내용은 Amazon Elastic Compute Cloud API 참조의 DescribeSecurityGroups를 참조하세요.

보안 그룹 규칙 수정

보안 그룹 규칙을 수정하여 액세스를 신뢰할 수 있는 특정 IP 주소 또는 범위로 제한합니다. 보안 그룹 규칙을 업데이트할 때는 각 필수 소스 IP 범위에 대한 규칙을 생성하거나 특정 포트에 대한 액세스를 제한하여 네트워크 세그먼트마다 액세스 요구 사항을 분리하는 것이 좋습니다. 보안 그룹 규칙을 수정하려면 Amazon EC2 사용 설명서의 보안 그룹 규칙 구성을 참조하세요. 기존 Amazon RDS 데이터베이스 인스턴스의 기본 포트를 수정하려면 Amazon Aurora 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하세요.

Amazon RDS DB 인스턴스에 IAM 데이터베이스 인증이 비활성화되어 있음

IAM 데이터베이스 인증을 사용하면 데이터베이스 암호 대신 IAM 자격 증명을 사용하여 Amazon RDS 데이터베이스에 인증할 수 있습니다. 이를 통해 중앙 집중식 액세스 관리, 임시 자격 증명, 애플리케이션 코드에 데이터베이스 암호를 저장할 필요 제거 등 몇 가지 보안 이점을 얻을 수 있습니다. IAM 데이터베이스 인증을 사용하면 암호 대신 인증 토큰을 사용하여 데이터베이스 인스턴스를 인증할 수 있습니다. 그 결과, 데이터베이스를 오가는 네트워크 트래픽은 SSL을 통해 암호화됩니다. IAM 인증을 사용하지 않으면 데이터베이스는 일반적으로 암호 기반 인증에 의존하므로 암호를 재사용하게 되고 암호가 약해질 수 있습니다. 보안 모범 사례에 따라 IAM 데이터베이스 인증을 활성화합니다.

문제 해결: IAM 데이터베이스 인증 활성화

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 DB 인스턴스가 열립니다. 데이터베이스 옵션에서 IAM 데이터베이스 인증을 활성화할 수 있습니다.

자세한 내용은 Amazon RDS 사용 설명서의 IAM 데이터베이스 인증 활성화 및 비활성화를 참조하세요. IAM 인증을 활성화한 후 암호 기반 인증 대신 IAM 인증을 사용하도록 DB 인스턴스를 업데이트합니다.

Amazon RDS DB 인스턴스가 기본 관리자 사용자 이름을 사용

DB 인스턴스에 기본 사용자 이름(예: “admin”, “root”)을 사용하면 무차별 대입 공격에서 널리 알려지고 일반적으로 대상으로 지정되므로 보안 위험이 증가합니다. 기본 사용자 이름은 예측 가능하며 권한이 없는 사용자가 더 쉽게 데이터베이스 액세스를 시도할 수 있습니다. 기본 사용자 이름을 사용하면 공격자가 데이터베이스에 액세스하는 데 둘 다 필요하지 않고 암호만 알아내면 됩니다. 보안 모범 사례에 따라 데이터베이스 인스턴스에 고유한 관리자 사용자 이름을 사용하여 모호성을 통해 보안을 강화하고 무단 액세스 시도의 위험을 줄입니다.

문제 해결: 고유한 관리자 사용자 이름 구성

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 DB 인스턴스가 열립니다. 기존 Amazon RDS DB 인스턴스의 관리자 사용자 이름은 변경할 수 없습니다. 고유한 관리

자 이름을 생성하려면 사용자 지정 사용자 이름으로 새 DB 인스턴스를 생성하고 데이터를 마이그레이션해야 합니다.

Amazon RDS DB 클러스터가 기본 관리자 사용자 이름을 사용

DB 인스턴스에 기본 사용자 이름(예: “admin”, “root”)을 사용하면 무차별 대입 공격에서 널리 알려지고 일반적으로 대상으로 지정되므로 보안 위험이 증가합니다. 기본 사용자 이름은 예측 가능하며 권한이 없는 사용자가 더 쉽게 데이터베이스 액세스를 시도할 수 있습니다. 기본 사용자 이름을 사용하면 공격자가 데이터베이스에 액세스하는 데 둘 다 필요하지 않고 암호만 알아내면 됩니다. 보안 모범 사례에 따라 데이터베이스 인스턴스에 고유한 관리자 사용자 이름을 사용하여 모호성을 통해 보안을 강화하고 무단 액세스 시도의 위험을 줄입니다.

문제 해결: 고유한 관리자 사용자 이름 구성

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 DB 인스턴스가 열립니다. 기존 Amazon RDS DB 인스턴스의 관리자 사용자 이름은 변경할 수 없습니다. 고유한 관리자 이름을 생성하려면 사용자 지정 사용자 이름으로 새 DB 인스턴스를 생성하고 데이터를 마이그레이션해야 합니다.

Amazon RDS DB 인스턴스에 마이너 버전 자동 업그레이드가 비활성화되어 있음

마이너 버전 자동 업그레이드를 사용하면 Amazon RDS 인스턴스는 마이너 엔진 버전 업그레이드가 릴리스되면 자동으로 업그레이드를 받을 수 있습니다. 이러한 업그레이드에는 데이터베이스의 보안 및 안정성을 유지하는 데 도움이 되는 중요한 보안 패치 및 버그 수정이 포함되는 경우가 많습니다. 데이터베이스가 최신 마이너 버전에서 수정된 알려진 보안 취약성으로 실행될 위험이 있습니다. 자동 업데이트를 사용하지 않으면 새 CVE가 발견됨에 따라 보안 취약성이 누적될 수 있습니다. 보안 모범 사례에 따라 모든 Amazon RDS 인스턴스에 대해 자동 마이너 버전 업그레이드를 활성화합니다.

문제 해결: 자동 마이너 버전 업그레이드 활성화

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 DB 인스턴스가 열립니다. 유지 관리 및 백업 탭에서 마이너 버전 자동 업그레이드 설정을 확인할 수 있습니다.

자세한 내용은 Amazon RDS for MySQL의 자동 마이너 버전 업그레이드를 참조하세요. 데이터베이스 활동이 적은 기간 동안 유지 관리 기간이 발생하도록 구성할 수도 있습니다.

Amazon RDS DB 인스턴스에 자동 백업이 비활성화되어 있음

자동 백업은 Amazon RDS 인스턴스에 대한 특정 시점 복구를 제공하므로 보존 기간 내의 어느 시점으로든 데이터베이스를 복원할 수 있습니다. 자동 백업이 비활성화되면 악의적인 삭제, 데이터 손상 또는

기타 데이터 손실 시나리오에서 데이터가 손실될 위험이 있습니다. 랜섬웨어 공격, 데이터베이스 테이블 삭제 또는 손상과 같은 악의적인 활동이 발생하는 경우 인시던트가 발생하기 전에 특정 시점으로 복원하는 기능은 인시던트 복구에 필요한 시간을 줄입니다. 보안 모범 사례에 따라 모든 프로덕션 데이터베이스에 대해 적절한 보존 기간으로 자동 백업을 활성화합니다.

Amazon RDS DB 인스턴스에 삭제 방지가 비활성화되어 있음

데이터베이스 삭제 방지는 데이터베이스 인스턴스의 삭제를 방지하는 데 도움이 되는 기능입니다. 삭제 방지를 비활성화하면 충분한 권한이 있는 모든 사용자가 데이터베이스를 삭제할 수 있으므로 데이터 손실 또는 애플리케이션 가동 중지가 발생할 수 있습니다. 공격자는 데이터베이스를 삭제하여 서비스 중단, 데이터 손실, 복구 시간 증가를 초래할 수 있습니다. 보안 모범 사례에 따라 RDS DB 인스턴스에 대한 삭제 방지를 활성화하여 악의적인 삭제를 방지합니다.

문제 해결: Amazon RDS DB 클러스터에 대한 삭제 방지 활성화

노출 결과에서 리소스 링크를 선택합니다. 그러면 영향을 받는 DB 클러스터가 열립니다.

Amazon RDS DB 클러스터에 삭제 방지가 비활성화되어 있음

데이터베이스 삭제 방지는 데이터베이스 인스턴스의 삭제를 방지하는 데 도움이 되는 기능입니다. 삭제 방지를 비활성화하면 충분한 권한이 있는 모든 사용자가 데이터베이스를 삭제할 수 있으므로 데이터 손실 또는 애플리케이션 가동 중지가 발생할 수 있습니다. 공격자는 데이터베이스를 삭제하여 서비스 중단, 데이터 손실, 복구 시간 증가를 초래할 수 있습니다. 보안 모범 사례에 따라 RDS DB 클러스터에 대한 삭제 방지를 활성화하여 악의적인 삭제를 방지합니다.

문제 해결: Amazon RDS DB 클러스터에 대한 삭제 방지 활성화

노출 결과에서 리소스 링크를 선택합니다. 그러면 영향을 받는 DB 클러스터가 열립니다.

Amazon RDS DB 인스턴스가 데이터베이스 엔진에 기본 포트를 사용

데이터베이스 엔진에 기본 포트를 사용하는 Amazon RDS 인스턴스는 보안 위험이 증가할 수 있습니다. 이러한 기본 포트는 널리 알려져 있으며 자동 스캔 도구의 표적이 되기 때문입니다. 기본 포트가 아닌 포트를 사용하도록 DB 인스턴스를 수정하면 모호성을 통해 보안 계층이 추가되므로 권한이 없는 사용자가 데이터베이스에 대한 자동 또는 표적 공격을 수행하기가 더 어려워집니다. 기본 포트는 일반적으로 권한이 없는 사람이 스캔하므로 이로 인해 DB 인스턴스가 표적이 될 수 있습니다. 보안 모범 사례에 따라 기본 포트를 사용자 지정 포트로 변경하여 자동 또는 대상 공격의 위험을 줄입니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

영향을 받는 리소스 업데이트

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 DB 인스턴스가 열립니다.

애플리케이션 연결 문자열 업데이트

포트를 변경한 후 새 포트 번호를 사용하도록 Amazon RDS 인스턴스에 연결하는 모든 애플리케이션 및 서비스를 업데이트합니다.

Amazon RDS DB 인스턴스가 백업 계획에 포함되지 않음

AWS Backup은 데이터 백업을 중앙 집중화하고 자동화하는 완전 관리형 백업 서비스입니다 AWS 서비스. DB 인스턴스가 백업 계획에 포함되지 않은 경우 악의적인 삭제, 데이터 손상 또는 기타 데이터 손실 시나리오에서 데이터가 손실될 위험이 있습니다. 랜섬웨어 공격, 데이터베이스 테이블 삭제 또는 손상과 같은 악의적인 활동이 발생하는 경우 인시던트가 발생하기 전에 특정 시점으로 복원하는 기능은 인시던트 복구에 필요한 시간을 줄입니다. 보안 모범 사례에 따라 Amazon RDS 인스턴스를 백업 계획에 포함시켜 데이터 보호를 보장합니다.

해결 방법: DB 인스턴스에 대한 백업 계획 생성 및 할당

노출 결과에서 리소스 링크를 선택합니다. 그러면 Amazon RDS 콘솔에서 영향을 받는 DB 인스턴스가 열립니다. 애플리케이션에 가장 적합한 백업 빈도, 보존 기간 및 수명 주기 규칙을 고려합니다.

Amazon RDS DB 인스턴스의 민감한 데이터 특성

다음은 Amazon RDS DB 인스턴스의 민감한 데이터 특성과 제안된 수정 단계입니다.

Amazon RDS DB 인스턴스에 민감한 데이터 포함

데이터 보안 스캔을 통해 Amazon RDS DB 인스턴스에 민감한 레코드가 있음을 확인했습니다. 통합 데이터 보안 제품은 DB 인스턴스의 콘텐츠를 검사하고 보호가 필요한 레코드를 식별할 때이 특성을 설정합니다.

민감한 데이터가 있으면 다른 모든 약점이 동일한 DB 인스턴스에 미치는 영향이 커집니다. 애플리케이션 데이터를 노출하는 네트워크 경로 또는 허용 액세스 구성은 규제 또는 기밀 레코드를 대신 노출합니다. DB 인스턴스에 도달하는 위협 행위자는 해당 레코드를 대량으로 쿼리 및 복사하여 환경 외부에 보관할 수 있습니다. 위협 행위자는 복구된 자격 증명을 사용하여 다른 시스템에 인증할 수도 있습니다. 보안 모범 사례에 따라 민감한 레코드를 저장하는 Amazon RDS DB 인스턴스에 대한 네트워크 및 자격 증명 액세스를 제한하고 저장 및 전송 중인 해당 레코드를 암호화하는 것이 좋습니다.

민감한 데이터에는 다음이 포함될 수 있습니다.

- 자격 증명 - 암호, 액세스 키, 연결 문자열 등
- 개인 식별 정보
- 금융 정보 - 계정 번호 및 결제 카드 데이터 등
- 보호가 필요한 기밀 콘텐츠

이 특성을 지우는 유일한 방법은 민감한 레코드를 제거하는 것입니다. 워크로드에서 DB 인스턴스에 민감한 데이터를 저장해야 하는 경우 다음 보안 모범 사례는 노출 위험을 줄입니다.

DB 인스턴스의 민감한 데이터 검토

노출 조사 결과에서 하이퍼링크를 사용하여 리소스를 엽니다. 그러면 영향을 받는 DB 인스턴스가 열립니다. DB 인스턴스 식별자를 기록하고 연결 및 보안 아래에 나열된 VPC 보안 그룹을 기록합니다. 민감한 레코드를 보고한 데이터 보안 조사 결과를 검토하여 해당 레코드를 포함하는 데이터베이스, 스키마 및 테이블을 결정합니다.

검색된 민감한 데이터의 유형에 따라 적절한 보안 제어를 구현합니다.

- 인바운드 네트워크 액세스 제한 - Amazon RDS 콘솔에서 데이터베이스를 선택하고 DB 인스턴스를 선택한 다음 연결 및 보안을 선택합니다. 연결된 각 VPC 보안 그룹을 열고 인바운드 규칙을 검토합니다. `0.0.0.0/0` 또는에서 데이터베이스 포트를 허용하는 규칙을 애플리케이션이 사용하는 특정 CIDR 범위 또는 보안 그룹 IDs`::/0`로 바꿉니다. 자세한 내용은 Amazon RDS 사용자 안내서의 보안 그룹을 통한 액세스 제어를 참조하세요.
- 퍼블릭 액세스 가능성 제거 - Amazon RDS 콘솔에서 DB 인스턴스를 선택하고 수정을 선택한 다음 연결에서 퍼블릭 액세스를 퍼블릭 액세스 불가로 설정합니다. 인터넷 게이트웨이로 라우팅되지 않는 프라이빗 서브넷에 DB 인스턴스를 배치합니다. VPC, AWS Direct Connect 또는 VPN 연결을 통해 애플리케이션에서 연결합니다. 자세한 내용은 Amazon RDS 사용 설명서의 VPC에서 DB 인스턴스를 사용한 작업을 참조하세요.
- 데이터베이스에 인증할 수 있는 사용자 제한 - 각 애플리케이션과 사용자에게 해당 함수에 필요한 데이터베이스 권한만 부여합니다. 필요하지 않은 데이터베이스 사용자의 민감한 레코드가 포함된 테이블에 대한 읽기 액세스를 취소합니다. IAM 데이터베이스 인증을 사용하면 IAM 자격 증명과 수명이 짧은 토큰이 수명이 긴 데이터베이스 암호 대신 액세스를 제어할 수 있습니다. 자세한 내용은 Amazon RDS 사용 설명서의 IAM 데이터베이스 인증을 참조하세요.
- 저장 시 민감한 레코드 암호화 - Amazon RDS 콘솔에서 DB 인스턴스를 선택하고 구성 탭을 선택하여 DB 인스턴스가 암호화를 사용하는지 확인합니다. 암호화되지 않은 기존 DB 인스턴스에서는 저장 시 암호화를 활성화할 수 없습니다. 데이터를 암호화하려면 DB 인스턴스의 스냅샷을 생성합니다.

스냅샷을 복사하고 복사할 AWS KMS 키를 선택한 다음 암호화된 스냅샷 복사본을 새 DB 인스턴스로 복원합니다. 새 엔드포인트에서 애플리케이션의 방향을 바꾸고 암호화되지 않은 DB 인스턴스와 스냅샷을 삭제합니다. 자세한 내용은 Amazon RDS 사용 설명서의 Amazon RDS 리소스 암호화를 참조하세요.

- 전송 중 암호화 필요 - Amazon RDS 인증서 번들을 사용하여 SSL/TLS에 연결하도록 데이터베이스 클라이언트를 구성합니다. 데이터베이스 엔진이 해당 목적으로 제공하는 파라미터를 통해 DB 인스턴스에 암호화된 연결을 적용합니다. 자세한 내용은 Amazon RDS 사용 설명서의 SSL/TLS를 사용하여 DB 인스턴스 또는 클러스터에 대한 연결 암호화를 참조하세요.
- DB 인스턴스에 대한 액세스 모니터링 - 데이터베이스 엔진 로그를 Amazon CloudWatch Logs에 게시하고 예상치 못한 소스의 연결과 민감한 레코드가 포함된 테이블에 대한 쿼리를 검토합니다. 자세한 내용은 Amazon RDS 사용 설명서의 Amazon RDS 로그 파일 모니터링을 참조하세요.

## Amazon S3 버킷에 대한 노출 문제 해결

AWS Security Hub는 Amazon Simple Storage Service(Amazon S3) 버킷에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Amazon S3 버킷 및 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침에 따라 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차

- Amazon S3 버킷의 잘못된 구성 특성
  - Amazon S3 버킷에서 버전 관리가 비활성화됨
  - Amazon S3 버킷에 Object Lock이 비활성화되어 있음
  - Amazon S3 버킷은 AWS KMS 키로 저장 시 암호화되지 않습니다.
  - 버전이 지정된 Amazon S3 버킷에서 다중 인증(MFA) 삭제가 비활성화됨
  - Amazon S3 버킷을 사용하면 다른 AWS 계정의 보안 주체가 버킷 권한을 수정할 수 있습니다.
- Amazon S3 버킷의 연결성 특성
  - Amazon S3 버킷에 퍼블릭 읽기 액세스가 있음
  - Amazon S3 버킷에는 퍼블릭 쓰기 액세스 권한이 있습니다.
- Amazon S3 버킷의 민감한 데이터 특성
  - Amazon S3 버킷에는 민감한 데이터가 포함되어 있습니다.


## Amazon S3 버킷의 잘못된 구성 특성

다음은 Amazon S3 버킷의 잘못된 구성 특성 및 제안된 문제 해결 단계입니다.

### Amazon S3 버킷에서 버전 관리가 비활성화됨

Amazon S3 버전 관리는 동일한 버킷 내에 여러 개의 객체 변형을 유지하는 데 도움이 됩니다. 버전 관리를 비활성화하면 Amazon S3는 각 객체의 최신 버전만 저장합니다. 즉, 객체가 실수로 또는 악의적으로 삭제되거나 덮어써지면 복구할 수 없습니다. 버전 관리가 활성화된 버킷은 우발적인 삭제, 애플리케이션 장애, 데이터 무단 수정 또는 삭제가 발생할 수 있는 랜섬웨어 공격과 같은 보안 사고로부터 보호됩니다. 보안 모범 사례에 따라 손실된 경우 다시 생성하기 어렵거나 불가능한 중요한 데이터가 포함된 버킷의 버전 관리를 활성화합니다.

#### 문제 해결: 버전 관리 활성화

버킷에서 Amazon S3 버전 관리를 활성화하려면 Amazon S3 사용 설명서의 버킷에서 버전 관리 활성화를 참조하세요. 버전 관리를 활성화할 때는 스토리지를 관리하기 위하 수명 주기 규칙을 구현하는 것이 좋습니다. 버전 관리는 객체의 여러 복사본을 유지 관리하기 때문입니다.

### Amazon S3 버킷에 Object Lock이 비활성화되어 있음

Amazon S3 Object Lock은 Amazon S3 객체에 대해 Write Once Read Many(WORM) 모델을 제공하므로, 객체가 고정 기간 동안 또는 무기한으로 삭제되거나 덮어쓰이지 않습니다. Object Lock이 비활성화되면 객체가 랜섬웨어에 의한 우발적이거나 악의적인 삭제, 수정 또는 암호화에 취약할 수 있습니다.

Object Lock은 변경 불가능한 데이터 스토리지가 필요한 규제 요구 사항을 준수하고 데이터 암호화를 시도할 수 있는 랜섬웨어와 같은 정교한 위협으로부터 보호하는 데 특히 중요합니다. Object Lock을 활성화하면 보존 정책을 추가된 데이터 보호 계층으로 적용하고 중요한 데이터에 대해 변경 불가능한 백업 전략을 생성할 수 있습니다. 보안 모범 사례에 따라 객체 잠금을 활성화하여 객체의 악의적인 수정을 방지합니다.

문제 해결: S3 객체 잠금 구성

Object Lock은 새 버킷을 생성할 때만 활성화할 수 있으므로 Object Lock이 활성화된 새 버킷을 생성해야 합니다. 대규모 마이그레이션의 경우 Batch Operations를 사용하여 객체를 새 버킷에 복사하는 것이 좋습니다. 객체를 잠그기 전에 버킷에 Amazon S3 버전 관리 및 Object Lock도 활성화해야 합니다. Object Lock은 새 버킷에서만 활성화할 수 있으므로 기존 데이터를 Object Lock이 활성화된 새 버킷으로 마이그레이션해야 합니다. 버킷에서 객체 잠금을 구성하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 객체 잠금 구성을 참조하세요. Amazon S3 Object Lock을 설정한 후 환경에 따라 적절한 보존 모드를 선택합니다.

Amazon S3 버킷은 AWS KMS 키로 저장 시 암호화되지 않습니다.

Amazon S3은 Amazon S3 관리형 키를 사용한 서버 측 암호화를 모든 새 버킷의 기본 암호화 수준으로 적용합니다. Amazon S3 관리형 키는 강력한 암호화 보호를 제공하지만 AWS Key Management Service 키와 동일한 수준의 액세스 제어 및 감사 기능을 제공하지 않습니다. KMS 키를 사용하는 경우 객체에 액세스하려면 Amazon S3 버킷과 객체를 암호화한 KMS 키 모두에 대한 권한이 필요합니다. 이는 암호화된 객체에 액세스할 수 있는 사용자를 세부적으로 제어해야 하고 암호화 키 사용에 대한 포괄적인 감사 로깅이 필요한 민감한 데이터에 특히 중요합니다. 보안 모범 사례에 따라 KMS 키를 사용하여 민감한 데이터가 포함된 버킷을 암호화하거나 엄격한 규정 준수 요구 사항이 있는 환경을 위해 암호화합니다.

문제 해결: S3 버킷 키 구성

새 객체에 Amazon S3 버킷 키를 사용하도록 버킷을 구성하려면 Amazon S3 사용 설명서의 새 객체에 SSE-KMS와 함께 Amazon S3 버킷 키를 사용하도록 버킷 구성을 참조하세요. Amazon S3 기존 객체를 암호화하는 방법에 대한 자세한 내용은 AWS 스토리지 블로그의 Amazon S3 배치 작업을 사용하여 객체 암호화를 참조하세요.

AWS KMS 암호화를 구현할 때는 다음 사항을 고려하세요.

- 키 관리 - AWS 관리형 키 또는 고객 관리형 키(CMK)를 사용할지 여부를 결정합니다. CMK를 사용하면 고객이 키의 수명 주기 및 사용을 완벽하게 제어합니다. 두 키 유형의 차이점에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS KMS 키를 참조하세요.

- 키 교체 - 추가 보안 조치를 위해 KMS 키에 대해 자동 키 교체를 활성화합니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 자동 키 교체 활성화를 참조하세요.

버전이 지정된 Amazon S3 버킷에서 다중 인증(MFA) 삭제가 비활성화됨

다중 인증(MFA) 삭제는 Amazon S3 버킷에 대한 추가 보안 계층을 제공합니다. 파괴적인 Amazon S3 작업을 위해서는 다중 인증이 필요합니다. MFA 삭제가 비활성화되면 적절한 권한이 있는 사용자는 추가 인증 문제 없이 버킷에서 객체 버전을 영구적으로 삭제하거나 버전 관리를 일시 중지할 수 있습니다. MFA 삭제를 활성화하면 데이터를 무단 또는 우발적 삭제로부터 보호하여 랜섬웨어 공격, 내부자 위협 및 운영 오류에 대한 보호를 강화할 수 있습니다. MFA 삭제는 무단 삭제로부터 보호해야 하는 중요하거나 규정 준수에 민감한 데이터가 포함된 버킷에 특히 유용합니다. 보안 모범 사례에 따라 Amazon S3 버킷에 대해 MFA를 활성화합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

MFA 유형 검토

AWS 는 다음과 같은 MFA 유형을 지원합니다. 물리적 디바이스를 사용한 인증은 일반적으로 더 엄격한 보안 보호를 제공하지만, 어떤 유형의 MFA를 사용해도 MFA를 비활성화하는 것보다 안전합니다.

리소스 정책 수준에서 MFA 적용

버킷 정책의 `aws:MultiFactorAuthAge` 조건 키를 사용하여 민감한 작업에 MFA를 요구합니다. 자세한 내용은 Amazon S3 사용 설명서의 MFA 요구하기를 참조하세요.

MFA 활성화

MFA 삭제를 활성화하려면 먼저 Amazon S3 버킷에서 버전 관리가 활성화되어 있어야 합니다. MFA 삭제는 버전 관리가 활성화된 버킷에서만 지원됩니다. Amazon S3 버전 관리를 활성화하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 버킷에서 버전 관리 활성화를 참조하세요. MFA 삭제는 Amazon S3 콘솔을 통해 활성화할 수 없습니다. Amazon S3 API 또는 AWS CLI를 사용해야 합니다. 자세한 내용은 Amazon S3 사용 설명서의 MFA 삭제 구성을 참조하세요.

Amazon S3 버킷을 사용하면 다른 AWS 계정의 보안 주체가 버킷 권한을 수정할 수 있습니다.

Amazon S3 버킷 리소스 정책은 버킷 및 객체에 대한 액세스를 제어합니다. 버킷 정책에서 다른 AWS 계정의 보안 주체가 버킷 권한을 수정하도록 허용하는 경우 권한이 없는 사용자는 버킷을 재구성할 수

있습니다. 외부 보안 주체 자격 증명이 손상되면 권한이 없는 사용자가 버킷을 제어하여 데이터 침해 또는 서비스 중단을 초래할 수 있습니다. 표준 보안 원칙에 따라 권한 관리 작업을 신뢰할 수 있는 보안 주체로만 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

버킷 정책 검토 및 식별

노출에서 ARN 필드에서 Amazon S3 버킷을 식별합니다. Amazon S3 콘솔에서 버킷을 선택하고 권한 탭으로 이동하여 버킷 정책을 검토합니다. 버킷에 연결된 권한 정책을 검토합니다. 위탁자 문에 표시된 대로 `s3:PutBucketPolicy, s3:PutBucketAcl, s3:DeleteBucketPolicy, s3:*` 과 같은 작업을 부여하는 정책 문 또는 계정 외부의 위탁자에게 액세스를 허용하는 정책 문을 찾습니다.

버킷 정책 수정

버킷 정책을 수정하여 다른 AWS 계정에 부여된 작업을 제거하거나 제한합니다.

- 외부 계정에 권한 관리 작업을 부여하는 정책 설명을 제거합니다.
- 교차 계정 액세스가 필요한 경우 광범위한 권한을 버킷 권한 관리가 포함되지 않은 특정 작업(`s3:*`)으로 바꿉니다.

버킷 정책을 수정하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조합니다.

Amazon S3 버킷의 연결성 특성

다음은 Amazon S3 버킷의 연결성 특성 및 제안된 문제 해결 단계입니다.

Amazon S3 버킷에 퍼블릭 읽기 액세스가 있음

퍼블릭 읽기 액세스를 사용하는 Amazon S3 버킷에서는 인터넷상의 모든 사용자가 버킷의 콘텐츠를 볼 수 있습니다. 공개적으로 액세스할 수 있는 웹 사이트 또는 공유 리소스에서는 이 액세스가 필요할 수 있지만 버킷에 민감한 데이터가 포함된 경우 보안 위험이 발생할 수 있습니다. 퍼블릭 읽기 액세스로 인해 무단 보기 및 다운로드가 발생할 수 있으며, 민감한 데이터가 해당 버킷에 저장되면 데이터 침해가 발생할 수 있습니다. 표준 보안 원칙에 따라 Amazon S3 버킷에 대한 액세스를 필요한 사용자 및 시스템으로 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

버킷 수준에서 퍼블릭 액세스 차단

Amazon S3는 버킷 정책 또는 ACL에 관계없이 퍼블릭 액세스를 방지하기 위해 버킷 수준 및 계정 수준 모두에서 구성할 수 있는 퍼블릭 액세스 차단 설정을 제공합니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하세요. Amazon S3 퍼블릭 액세스를 차단한 후 버킷 액세스 제어 구성을 검토하여 액세스 요구 사항에 부합하는지 확인합니다. 그런 다음 Amazon S3 버킷 정책을 검토하여 버킷에 액세스할 수 있는 사용자를 명시적으로 정의합니다. 버킷 정책의 예는 Amazon S3 사용 설명서의 Amazon S3 버킷 정책 예제를 참조하세요. Amazon S3

대체 액세스 방법

퍼블릭 읽기 액세스가 필요한 경우 다음과 같은 보다 안전한 대안을 고려할 수 있습니다.

- Amazon CloudFront - CloudFront를 오리진 액세스 ID(OAI) 또는 오리진 액세스 제어(OAC)와 함께 사용하여 프라이빗 Amazon S3 버킷에서 읽기 액세스를 허용합니다. 이 대안은 CloudFront를 통해 콘텐츠에 공개적으로 액세스할 수 있도록 허용하면서 Amazon S3 버킷에 대한 직접 액세스를 제한합니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하세요.
- 미리 서명된 URL - 특정 객체에 대한 임시 액세스를 위해 미리 서명된 URL을 사용합니다. 자세한 내용은 Amazon S3 사용 설명서의 미리 서명된 URLs.

Amazon S3 버킷에는 퍼블릭 쓰기 액세스 권한이 있습니다.

퍼블릭 쓰기 액세스를 사용하는 Amazon S3 버킷에서는 인터넷상의 모든 사용자가 버킷의 객체를 업로드, 수정 또는 삭제할 수 있습니다. 이로 인해 누군가 악성 파일을 업로드하고, 기존 파일을 수정하고, 데이터를 삭제할 수 있는 가능성을 포함하여 상당한 보안 위험이 발생합니다. 퍼블릭 쓰기 액세스는 공격자가 악용할 수 있는 보안 취약성을 생성합니다. 표준 보안 원칙에 따라 Amazon S3 버킷에 대한 쓰기 액세스를 필요한 사용자 및 시스템으로만 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

계정 및 버킷 수준에서 퍼블릭 액세스 차단

Amazon S3는 버킷 정책 또는 ACL에 관계없이 퍼블릭 액세스를 방지하기 위해 버킷 수준 및 계정 수준 모두에서 구성할 수 있는 퍼블릭 액세스 차단 설정을 제공합니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하세요. Amazon S3

버킷 정책 수정

퍼블릭 쓰기 액세스를 제거하는 보다 세분화된 접근 방식을 사용하려면 버킷 정책을 검토하세요. `s3:PutObject`, `s3:DeleteObject` 또는 `s3:*`을 찾을 수 있습니다. 버킷 정책 관리에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3에 대한 버킷 정책을 참조하세요. Amazon S3

대체 액세스 방법

퍼블릭 쓰기 액세스가 필요한 경우 다음과 같은 보다 안전한 대안을 고려하세요.

- 미리 서명된 URL - 특정 객체에 대한 임시 액세스를 위해 미리 서명된 URL을 사용합니다. 자세한 내용은 Amazon S3 사용 설명서의 미리 서명된 URLs.
- Amazon API Gateway 프록시 -에서 API Gateway와 같은 중개자를 사용하여 Amazon S3 버킷 AWS Lambda 에 쓰기 전에 요청을 검증하고 승인합니다. 이 접근 방식은 클라이언트가 버킷에 직접 쓰지 않도록 합니다. 자세한 내용은 API Gateway 개발자 안내서의 자습서: Amazon S3 프록시로 REST API 생성을 참조하세요.
- Amazon CloudFront - 항상 요청에 서명하도록 구성된 오리진 액세스 제어(OAC)와 함께 CloudFront를 사용합니다. PUT 및 POST 메서드를 활성화하여 Amazon S3 버킷을 직접 노출하지 않고 인증된 쓰기를 허용합니다. 권한이 없는 사용자가 유지하려는 객체를 삭제할 수 없도록 권한이 부여된 보안 주체로만 `s3:DeleteObject` 권한을 제한하도록 버킷 정책을 구성합니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한 섹션을 참조하세요.

Amazon S3 버킷의 민감한 데이터 특성

다음은 Amazon S3 버킷의 민감한 데이터 특성 및 제안된 문제 해결 단계입니다.

Amazon S3 버킷에는 민감한 데이터가 포함되어 있습니다.

데이터 보안 스캔에서 민감한 데이터가 Amazon S3 버킷에 존재하는 것으로 확인되었습니다. 통합 데이터 보안 제품은 버킷의 객체를 검사하고 보호가 필요한 콘텐츠를 식별할 때이 특성을 설정합니다. Security Hub는 검사를 수행한 제품에 관계없이 동일한 방식으로 특성을 보고합니다.

민감한 데이터에는 다음이 포함될 수 있습니다.

- 자격 증명
- 개인 식별 정보
- 금융 정보
- 보호가 필요한 기밀 콘텐츠

구성 오류 또는 무단 액세스를 통해 민감한 데이터가 노출되면 규정 준수 위반, 데이터 침해, ID 도용 또는 재정적 손실이 발생할 수 있습니다. 보안 모범 사례에 따라 데이터를 적절하게 분류하고 Amazon S3 버킷의 민감한 데이터를 지속적으로 모니터링하세요.

문제 해결

이 특성을 지우려면 버킷에서 민감한 데이터를 제거합니다. 워크로드에서 버킷에 민감한 데이터를 저장해야 하는 경우 다음 보안 제어를 구현하여 노출 위험을 줄입니다.

버킷의 민감한 데이터 검토

노출 결과에서 리소스 열기를 선택합니다. 민감한 데이터를 보고한 데이터 보안 조사 결과를 검토하여 민감한 데이터가 포함된 객체 또는 접두사를 결정합니다. Macie에서 탐지한 경우 결과 유형은 민감한 데이터의 범주를 설명합니다. 자세한 내용은 Amazon Macie Macie 사용 설명서의 Macie 조사 결과 유형을 참조하세요.

검색된 민감한 데이터의 유형에 따라 적절한 보안 제어를 구현합니다.

- 버킷에 대한 액세스 제한 - 버킷 권한을 검토하여 최소 권한 원칙을 준수하는지 확인합니다. IAM 정책, 버킷 정책 및 ACL을 사용하여 액세스를 제한합니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3의 Identity and Access Management를 참조하세요. Amazon S3
- 서버 측 암호화 활성화 - 추가 보호를 위해 KMS 키로 서버 측 암호화를 활성화합니다. 자세한 내용은 Amazon S3 사용 설명서의 AWS KMS 키를 사용한 서버 측 암호화(SSE-KMS) 사용을 참조하세요.
- 민감한 데이터 수정 또는 변환 - 객체가 민감한 값을 유지할 필요가 없는 경우 AWS Glue DataBrew를 사용하여 데이터를 준비합니다. 다운스트림 시스템이 데이터를 사용하기 전에 해당 값을 제거하는 마스킹, 교체 또는 해싱 변환을 적용합니다. 준비된 출력을 자체 액세스 제어가 있는 별도의 버킷에 씁니다. 자세한 내용은 AWS Glue DataBrew 개발자 가이드의 AWS Glue DataBrew이란 무엇입니까?를 참조하세요.

## Amazon SageMaker 노트북 인스턴스에 대한 노출 문제 해결

AWS Security Hub는 Amazon SageMaker 노트북 인스턴스에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서는 노출 조사 결과와 관련된 노트북 인스턴스와 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경

우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침은 다른 AWS 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Amazon SageMaker 노트북 인스턴스의 구성 오류 특성
  - Amazon SageMaker 노트북 인스턴스에 직접 인터넷 액세스가 활성화되어 있음
  - Amazon SageMaker 노트북 인스턴스에 루트 액세스가 활성화되어 있음
- Amazon SageMaker 노트북 인스턴스의 민감한 데이터 특성
  - Amazon SageMaker 노트북 인스턴스에 민감한 데이터 포함
- Amazon SageMaker 노트북 인스턴스의 영향 특성
  - 전체 제어 권한 있는 실행기 경로 보유
  - 직접 정책 에스컬레이션 경로가 있음
  - 신뢰 정책 하이재크 경로가 있음
  - 데이터 랜섬웨어 경로가 있음
  - 제한 경로 제거
  - 패스 역할 생성 실행기 경로가 있음
  - 스왑 역할 기존 실행기 경로가 있음
  - 역할 체인 에스컬레이션 경로가 있음
  - 코드 삽입 권한이 있는 실행기 경로가 있음
  - 감사 추적 경로 비활성화
  - 기존 실행기 경로에 액세스할 수 있음
  - 자격 증명 마이닝 경로가 있음
  - 패스 역할 데이터 액세스 경로가 있음
  - 역할 전달 작업 하이재크 경로가 있음

- 단일 홉 데이터 액세스 경로가 있음
- 기능 발전 경로가 있음

Amazon SageMaker 노트북 인스턴스의 구성 오류 특성

다음은 Amazon SageMaker 노트북 인스턴스의 잘못된 구성 특성과 제안된 수정 단계입니다.

Amazon SageMaker 노트북 인스턴스에 직접 인터넷 액세스가 활성화되어 있음

Amazon SageMaker 노트북 인스턴스에서를 `DirectInternetAccess` 활성화하면 아웃바운드 트래픽이 SageMaker 관리형 네트워크 주소 변환(NAT) 게이트웨이를 통해 인터넷으로 라우팅됩니다. 이렇게 하면 데이터 유출에 사용하거나 노트북이 손상된 경우 command-and-control 채널로 사용할 수 있는 송신 경로가 제공됩니다. 보안 모범 사례에 따라 직접 인터넷 액세스를 비활성화하고 필요한 AWS 서비스를 위해 VPC 엔드포인트가 있는 VPC에 노트북 인스턴스를 배치합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

직접 인터넷 액세스 비활성화

노트북 인스턴스를 생성한 후에는 `DirectInternetAccess` 설정을 변경할 수 없습니다. 비활성화하려면 VPC 내의 프라이빗 서브넷`Disabled`에서가 로 `DirectInternetAccess` 설정된 새 노트북 인스턴스를 생성한 다음 기존 인스턴스에서 노트북과 데이터를 마이그레이션합니다. 지침은 Amazon SageMaker 개발자 안내서의 VPC의 노트북 인스턴스를 외부 리소스에 연결을 참조하세요.

VPC 엔드포인트 구성

직접 인터넷 액세스를 비활성화하면 Amazon S3 및 Amazon SageMaker API와 같은 AWS 서비스에 액세스하려면 노트북 인스턴스에 VPC 엔드포인트가 필요합니다. 노트북에 필요한 서비스에 대한 인터페이스 VPC 엔드포인트를 생성합니다. VPC 엔드포인트에 대한 자세한 내용은 What is AWS PrivateLink?를 참조하세요. AWS PrivateLink 안내서의 .

Amazon SageMaker 노트북 인스턴스에 루트 액세스가 활성화되어 있음

Amazon SageMaker 노트북 인스턴스에서를 `RootAccess` 활성화하면 사용자에게 전체 OS 수준 루트 권한이 부여됩니다. 루트 액세스는 임의의 시스템 수정, 영구 백도어 및 무제한 패키지 설치를 허용합니다. 보안 모범 사례에 따라 워크플로에 명시적으로 필요하지 않은 한 노트북 인스턴스에 대한 루트 액세스를 비활성화합니다.

문제 해결: 루트 액세스 비활성화

실행 중인 노트북 인스턴스에서는 RootAccess 설정을 변경할 수 없습니다. 비활성화하려면 인스턴스를 중지한 다음 인스턴스 구성을 업데이트하여를 RootAccess로 설정합니다Disabled. 를 사용한 패키지 설치 pip 및 수명 주기 구성 실행을 포함한 대부분의 노트북 워크플로는 루트 액세스 없이 계속 작동합니다. 지침은 Amazon SageMaker 개발자 안내서의 Amazon SageMaker 노트북 인스턴스에 대한 루트 액세스 제어를 참조하세요. Amazon SageMaker

추가 고려 사항

특정 작업에 루트 액세스가 필요한 경우 Amazon SageMaker Studio 노트북을 대신 사용하는 것이 좋습니다.이 노트북은 격리된 컨테이너 기반 환경에 보다 세분화된 액세스 제어를 제공합니다. 수명 주기 구성을 사용하여 인스턴스 생성 시 필요한 패키지를 사전 설치하여 정상적인 사용 중에 루트 액세스의 필요성을 줄일 수도 있습니다.

Amazon SageMaker 노트북 인스턴스의 민감한 데이터 특성

다음은 Amazon SageMaker 노트북 인스턴스의 민감한 데이터 특성과 제안된 수정 단계입니다.

Amazon SageMaker 노트북 인스턴스에 민감한 데이터 포함

데이터 보안 스캔을 통해 Amazon SageMaker 노트북 인스턴스에 민감한 데이터가 있음을 확인했습니다. 통합 데이터 보안 제품은이 특성을 설정합니다. 제품은 노트북 파일, 출력 및 연결된 스토리지를 검사하고 보호가 필요한 콘텐츠를 식별합니다. 검사를 수행한 통합 제품에 관계없이 Security Hub에서이 특성을 일관되게 보고합니다.

민감한 데이터는 다른 모든 약점이 동일한 노트북 인스턴스에 미치는 영향을 높입니다. 허용 실행 역할, 직접 인터넷 송신 경로 또는 지나치게 광범위한 액세스는 규제되거나 기밀인 콘텐츠를 노출합니다. 노트북에 도달하는 위협 행위자는 노트북 파일, 출력 셀 및 저장된 체크포인트에서 해당 레코드를 읽고 복사할 수 있습니다. 그러면 위협 행위자는 이러한 레코드를 환경 외부에 보관할 수 있습니다. 노트북에 있는 모든 자격 증명을 사용하여 다른 시스템에 인증할 수도 있습니다.

보안 모범 사례에 따라 민감한 데이터를 보유한 노트북 인스턴스에 대한 액세스를 제한하고 연결된 저장 스토리지를 암호화하는 것이 좋습니다.

민감한 데이터에는 다음이 포함될 수 있습니다.

- 자격 증명 - 암호, 액세스 키, 연결 문자열 등
- 개인 식별 정보

- 금융 정보 - 계정 번호 및 결제 카드 데이터 등
- 보호가 필요한 기밀 콘텐츠

노트북에서 민감한 데이터를 제거하는 것이이 특성을 지우는 유일한 방법입니다. 노트북이 민감한 데이터를 참조해야 하는 경우 다음 보안 모범 사례는 노출 위험을 줄입니다.

노트북 인스턴스에서 민감한 데이터 검토

노출 조사 결과에서 하이퍼링크를 사용하여 리소스를 엽니다. 그러면 영향을 받는 노트북 인스턴스가 열립니다. 노트북 인스턴스 이름, AWS 계정 및 AWS 리전을 기록해 둡니다. 민감한 데이터를 보고한 데이터 보안 조사 결과를 검토하여 이를 포함하는 노트북 파일, 출력 셀 또는 체크포인트를 결정합니다.

검색된 민감한 데이터의 유형에 따라 적절한 보안 제어를 구현합니다.

- 노트북에서 민감한 값 제거 - 노트북 코드에서 민감한 값을 삭제하고 해당 값이 포함된 출력 셀을 지웁니다. 값을 유지하는 저장된 체크포인트와 내보낸 복사본을 모두 삭제합니다. 값을 참조된 상태로 유지해야 하는 경우 토큰화되거나 마스킹 처리된 자리 표시자로 바꿉니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 Amazon SageMaker 노트북 인스턴스 사용을 참조하세요. Amazon SageMaker
- 노출된 자격 증명 교체 - 노트북에 자격 증명이 포함된 경우 해당 자격 증명을 손상된 것으로 취급합니다. 자격 증명을 비활성화하고 교체한 다음 영향을 받는 시스템의 감사 로그를 검토하여 노출된 값을 사용합니다. 노트북 콘텐츠에 임베딩하는 대신 범위가 좁은 실행 역할을 AWS Secrets Manager 통해에서 런타임 시 보안 암호를 검색합니다. 자세한 내용은 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 보안 암호 교체를 참조하세요.
- 노트북 인스턴스를 열 수 있는 사용자 제한 - 노트북 인스턴스가 필요한 IAM 자격 증명에만 액세스 권한을 부여합니다. 실행 역할의 범위를 노트북이 사용하는 특정 작업 및 리소스로 지정합니다. `sagemaker:CreatePresignedNotebookInstanceUrl` 권한을 제한하여 노트북을 열 수 있는 사용자를 제어합니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 Amazon SageMaker 자격 증명 기반 정책 예제를 참조하세요. Amazon SageMaker
- 저장된 노트북 스토리지 암호화 - 노트북 파일 및 체크포인트를 보관하는 스토리지 볼륨이 저장 시 암호화되도록 노트북 인스턴스에 AWS KMS 키를 연결합니다. 키 정책을 제어할 수 있도록 고객 관리형 키를 사용합니다. 노트북을 읽어야 하는 자격 증명에만 `kms:Decrypt` 해당 키를 부여합니다. 자세한 내용은 Amazon SageMaker 개발자 안내서의 암호화를 사용하여 저장 데이터 보호를 참조하세요.
- 노트북 인스턴스에 대한 액세스 모니터링 - `sagemaker:CreatePresignedNotebookInstanceUrl` 호출 및 예상치 못한 ID 또는 소스의 액

세스를 검토합니다. AWS CloudTrail 자세한 내용은 Amazon SageMaker 개발자 안내서의를 사용하여 Amazon SageMaker API 호출 로깅 AWS CloudTrail을 참조하세요. Amazon SageMaker

Amazon SageMaker 노트북 인스턴스의 영향 특성

영향 특성은 노출의 잠재적 폭발 반경을 설명합니다. Security Hub는 SageMaker 노트북 인스턴스와 연결된 AWS Identity and Access Management 보안 주체의 유효 권한을 분석하여 노트북 인스턴스가 손상된 경우 공격자가 도달할 수 있는 다운스트림 리소스를 결정합니다. 각 영향 특성은 특정 권한 에스컬레이션 패턴을 식별합니다. 블래스트 반경을 줄이려면 각 특성에 설명된 권한 경로를 검토하고 불필요한 권한을 제거합니다.

표준 보안 원칙에 따라 작업을 수행하는 데 필요한 권한만 제공하여 최소 권한을 부여합니다. 광범위한 정책을 필요한 특정 작업 및 리소스만 부여하는 범위 축소 정책으로 바꿉니다. 제거할 미사용 권한을 식별하려면 IAM Access Analyzer를 사용하여 액세스 기록을 기반으로 권장 사항을 생성합니다. 자세한 내용은 IAM 사용 설명서의 외부 및 미사용 액세스 결과 및 최소 권한 적용을 참조하세요.

전체 제어 권한 있는 실행기 경로 보유

연결된 보안 주체는 이미 승격된 권한이 있는 컴퓨팅 리소스에 역할을 전달하고 코드를 주입할 수 있습니다. 이를 통해 보안 주체는 실행기를 완전히 제어하고 실행기의 역할이 허용하는 모든 작업을 수행할 수 있습니다.

직접 정책 에스컬레이션 경로가 있음

연결된 보안 주체는 IAM 정책을 직접 수정하여 추가 권한을 부여하고 중간 리소스 없이 자체 권한을 에스컬레이션할 수 있습니다.

신뢰 정책 하이재크 경로가 있음

연결된 보안 주체는 IAM 역할의 신뢰 정책을 수정하여가 해당 역할을 수임하여 역할의 권한을 얻도록 허용할 수 있습니다.

데이터 랜섬웨어 경로가 있음

연결된 보안 주체는 고객 관리형 AWS KMS 키로 Amazon S3 객체를 암호화한 다음 키 정책을 수정하는 등 랜섬웨어에 사용할 수 있는 방식으로 데이터를 암호화하거나 삭제할 수 있습니다.

제한 경로 제거

연결된 보안 주체는 권한 경계, 서비스 제어 정책 또는 리소스 기반 정책 거부 문과 같은 보안 제한을 제거하여 다른 보안 주체 또는 리소스 자체가 수행할 수 있는 작업을 확장할 수 있습니다.

패스 역할 생성 실행기 경로가 있음

연결된 보안 주체는 새 컴퓨팅 리소스(예: Lambda 함수 또는 Amazon EC2 인스턴스)를 생성하고 권한 있는 역할을 전달하여 새 리소스를 통해 자체 권한을 효과적으로 로세싱할 수 있습니다.

스왑 역할 기존 실행기 경로가 있음

연결된 보안 주체는 기존 컴퓨팅 리소스에 연결된 IAM 역할을 변경하여 더 권한이 있는 역할로 대체하여 액세스를 에스컬레이션할 수 있습니다.

역할 체인 에스컬레이션 경로가 있음

연결된 보안 주체는 일련의 역할을 수임할 수 있습니다. 여기서 체인의 각 역할은 점진적으로 더 광범위한 권한을 가지므로 궁극적으로 권한이 높은 역할에 도달합니다.

코드 삽입 권한이 있는 실행기 경로가 있음

연결된 보안 주체는 권한이 승격된 실행 중인 컴퓨팅 리소스에 코드를 주입하여 해당 리소스의 권한 있는 역할에 따라 임의 작업을 실행할 수 있습니다.

감사 추적 경로 비활성화

연결된 보안 주체는 CloudTrail과 같은 로깅 또는 모니터링 서비스를 비활성화하여 에스컬레이션 중 또는 에스컬레이션 후에 트랙을 효과적으로 처리할 수 있습니다.

기존 실행기 경로에 액세스할 수 있음

연결된 보안 주체는 기존 컴퓨팅 리소스를 호출하거나 연결하고 연결된 역할을 사용하여 권한 있는 작업을 수행할 수 있습니다.

자격 증명 마이닝 경로가 있음

연결된 보안 주체는 다른 보안 주체에 대한 새 장기 자격 증명(예: 액세스 키 또는 로그인 프로필)을 생성하여 암호 교체 또는 세션 만료 후에도 지속되는 영구 액세스 경로를 설정할 수 있습니다.

패스 역할 데이터 액세스 경로가 있음

연결된 보안 주체는 서비스 리소스를 생성하고 민감한 데이터에 액세스할 수 있는 역할을 전달하여 새 리소스를 통해 해당 데이터에 간접적으로 액세스할 수 있습니다.

역할 전달 작업 하이재크 경로가 있음

연결된 보안 주체는 예약된 작업 또는 이벤트 기반 작업(예: 이벤트에 의해 트리거된 Lambda 함수)에 역할을 전달하여 해당 역할의 권한으로 임의의 코드를 실행할 수 있습니다.

단일 홉 데이터 액세스 경로가 있음

연결된 보안 주체는 중간 에스컬레이션 단계 없이 기존 권한을 통해 민감한 데이터 리소스(예: Amazon S3 버킷 또는 DynamoDB 테이블)에 직접 액세스할 수 있습니다.

기능 발전 경로가 있음

연결된 보안 주체에는 직접 할당된 권한 이상으로 전체 기능을 발전시키는 권한 에스컬레이션 경로가 있습니다. 이는 보다 구체적인 패턴과 일치하지 않는 경로에 대한 일반적인 분류입니다.

## Azure 가상 머신에 대한 노출 문제 해결

AWS Security Hub는 Azure 가상 머신에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서는 노출 조사 결과와 관련된 Azure 가상 머신과 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 수정 지침에 따라 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure 가상 머신의 구성 오류 특성
  - Azure 가상 머신에는 개방형 네트워크 보안 그룹이 있습니다.
  - Azure 가상 머신에는 SSH 또는 RDP 액세스를 허용하는 보안 규칙이 있습니다.
  - Azure 가상 머신과 연결된 역할에 관리 액세스 역할 할당이 있습니다.

  - Azure 가상 머신에는 end-of-life 운영 체제가 있습니다.
- Azure 가상 머신의 연결성 특성
  - Azure 가상 머신은 인터넷을 통해 연결할 수 있습니다.
- Azure 가상 머신의 취약성 특성
  - Azure 가상 머신에는 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있습니다.
  - Azure 가상 머신에 소프트웨어 취약성이 있음
  - Azure 가상 머신에 악성 소프트웨어 패키지가 있음

Azure 가상 머신의 구성 오류 특성

다음은 Azure 가상 머신의 잘못된 구성 특성과 제안된 수정 단계입니다.

Azure 가상 머신에는 개방형 네트워크 보안 그룹이 있습니다.

네트워크 보안 그룹(NSG)은 Azure 가상 머신의 가상 방화벽 역할을 하여 우선 순위가 지정된 보안 규칙 세트로 인바운드 및 아웃바운드 트래픽을 필터링합니다. 개방형 네트워크 보안 그룹에는 모든 소스(예: Any 또는 소스)에서 무제한 액세스를 허용하는 규칙이 포함되어 있습니다`0.0.0.0/0`. 이러한 규칙은 가상 머신을 인터넷에서 무단 액세스에 노출시킬 수 있습니다. 표준 보안 원칙에 따라 네트워크 보안 그룹 규칙을 워크로드에 필요한 특정 IP 주소, 포트 및 프로토콜로만 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

네트워크 보안 그룹 규칙 검토 및 현재 구성 평가

가상 머신의 네트워크 인터페이스 또는 서브넷과 연결된 네트워크 보안 그룹을 식별하고 인바운드 보안 규칙을 검토합니다. Any 또는와 같은 광범위한 소스 범위의 트래픽을 허용하는 포트를 평가합니다`0.0.0.0/0`. 규칙은 우선 순위에 따라 처리되므로 허용 규칙이 보다 제한적인 규칙보다 우선하지 않는지 확인합니다. 자세한 내용은 Microsoft Azure 설명서의 네트워크 보안 그룹을 참조하세요.

네트워크 보안 그룹 규칙 제한

무제한 액세스를 허용하는 규칙을 수정하거나 제거합니다. 와 같은 광범위한 소스를 액세스가 필요한 신뢰할 수 있는 Any 특정 IP 주소, CIDR 범위, 서비스 태그 또는 애플리케이션 보안 그룹으로 바꿉니다. 대상 포트 범위를 워크로드가 사용하는 포트로만 제한합니다. 자세한 내용은 Microsoft Azure 설명서의 네트워크 보안 그룹 관리를 참조하세요.

Azure 가상 머신에는 SSH 또는 RDP 액세스를 허용하는 보안 규칙이 있습니다.

SSH(포트 22) 및 RDP(포트 3389)와 같은 원격 관리 프로토콜을 사용하면 사용자가 원격 위치에서 Azure 가상 머신에 연결하고 관리할 수 있습니다. 네트워크 보안 그룹 규칙이 인터넷( Any 또는 소스`0.0.0.0/0`)에서 이러한 포트를 허용하면 가상 머신의 공격 표면이 크게 증가하여 무차별 대입 및 보안 인증 기반 공격에 노출됩니다. 표준 보안 원칙에 따라 신뢰할 수 있는 특정 IP 주소로 원격 액세스를 제한하거나 이러한 포트에 대한 직접 인터넷 액세스를 완전히 제거합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

네트워크 보안 그룹 규칙 제한

SSH 및 RDP 액세스를 대신 신뢰할 수 있는 특정 IP 주소 또는 CIDR 범위로 제한Any하거나 인터넷에서 원격 액세스가 필요하지 않은 경우 인바운드 규칙을 제거합니다. 자세한 내용은 Microsoft Azure 설명서의 네트워크 보안 그룹 관리를 참조하세요.

Azure Bastion을 사용하여 보안 연결

SSH 또는 RDP 포트를 인터넷에 노출하는 대신 Azure Bastion을 사용하여 퍼블릭 IP 주소나 열린 인바운드 포트 없이 TLS를 통해 가상 머신에 연결합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure Bastion을 참조하세요.

just-in-time 가상 머신 액세스 사용

Microsoft Defender for Cloud에서 just-in-time(JIT) 가상 머신 액세스를 활성화하여 SSH 및 RDP와 같은 관리 포트가 기본적으로 닫혀 있고 지정된 소스 IP 주소의 승인된 시간 제한 요청에 대해서만 열려 있도록 합니다. 자세한 내용은 Microsoft Azure 설명서의 just-in-time 액세스 활성화를 참조하세요.

Azure 가상 머신과 연결된 역할에 관리 액세스 역할 할당이 있습니다.

Azure 가상 머신에 관리형 자격 증명을 할당하고 다른 Azure 리소스에 액세스할 수 있도록 Azure 역할 기반 액세스 제어(Azure RBAC) 역할 할당을 부여할 수 있습니다. 연결된 자격 증명에 광범위한 범위의 관리 역할 할당(예: `Owner` 또는 `Contributor`)이 있는 경우 일반적으로 워크로드에 필요한 것 이상의 권한을 부여합니다. 가상 머신이 손상된 경우 공격자는 이러한 과도한 권한을 사용하여 환경 전체에서 내부적으로 이동하거나, 데이터에 액세스하거나, 리소스를 조작할 수 있습니다. 표준 보안 원칙에 따라 워크로드에 필요한 권한만 할당하여 최소 권한을 부여합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

관리 역할 할당 검토 및 식별

Azure 포털에서 가상 머신과 연결된 자격 증명에 대한 역할 할당을 검토합니다. `Owner`에서 와일드카드(*)를 사용하는 사용자 지정 역할에 대해 `User Access Administrator`, `Contributor`또는와 같은 권한이 있는 관리자 역할을 찾습니다`Actions`. 자세한 내용은 Microsoft Azure 설명서의 Azure 역할 할당 나열을 참조하세요.

최소 권한 액세스 구현

관리 역할 할당을 워크로드에 필요한 권한만 부여하는 최소 권한의 기본 제공 역할로 바꿉니다. 필요에 맞는 가장 좁은 범위(리소스 또는 리소스 그룹)에 할당합니다. 사용자 지정 역할을 생성할 때 와일드카드를 사용하는 대신 `Actions` 및를 `DataActions` 명시적으로 지정합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure RBAC 모범 사례를 참조하세요.

Azure 가상 머신에는 end-of-life 운영 체제가 있습니다.

Azure 가상 머신은 공급업체가 더 이상 지원하지 않거나 유지 관리하지 않는 end-of-life 운영 체제를 실행합니다. 운영 체제의 수명이 다하면 공급업체는 보안 업데이트 및 권고 릴리스를 중지합니다. 그러면 알려진 취약성이 영구적으로 패치되지 않고 가상 머신이 공격에 노출됩니다. 보안 모범 사례에 따라 지원되는 운영 체제 버전으로 업그레이드합니다.

문제 해결: 지원되는 운영 체제 버전으로 업그레이드

현재 위치 업그레이드를 계획하거나 지원되는 운영 체제 버전을 실행하는 가상 머신으로 워크로드를 마이그레이션합니다. 업그레이드하기 전에 애플리케이션 호환성을 확인하고 필요한 경우 롤백할 수 있도록 백업 또는 스냅샷을 생성합니다. Windows의 경우 현재 위치 업그레이드 지침을 따르고, Linux의 경우 배포 공급업체의 업그레이드 지침을 따릅니다. 자세한 내용은 Microsoft Azure 설명서의 Windows Server VM의 현재 위치 업그레이드 수행을 참조하세요.

Azure 가상 머신의 연결성 특성

다음은 Azure 가상 머신의 연결성 특성과 제안된 문제 해결 단계입니다.

Azure 가상 머신은 인터넷을 통해 연결할 수 있습니다.

인터넷에서 연결할 수 있는 포트가 있는 Azure 가상 머신은 공격에 노출될 수 있습니다. 퍼블릭 IP 주소가 있으면 가상 머신에 연결할 수 있습니다. 또한 로드 밸런서, 애플리케이션 게이트웨이 또는 기타 네트워크 경로가 인터넷으로부터의 인바운드 트래픽을 허용하는 경우에도 연결할 수 있습니다. 표준 보안 원칙에 따라 인바운드 트래픽을 필요한 소스 및 포트로만 제한하여 최소 권한 네트워크 액세스 제어를 구현합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

인터넷 노출 제한 또는 제거

가상 머신에 퍼블릭 IP 주소가 필요한지 검토합니다. 그렇지 않은 경우 네트워크 인터페이스에서 퍼블릭 IP 주소의 연결을 해제하고 대신 프라이빗 IP 주소를 사용합니다. 아웃바운드 인터넷 연결이 여전히 필요한 경우 NAT 게이트웨이를 사용합니다.

인바운드 액세스가 필요한 경우 가상 머신을 직접 노출하는 대신 로드 밸런서, Azure 방화벽 또는 애플리케이션 게이트웨이 뒤에 배치합니다. 자세한 내용은 Microsoft Azure 설명서의 퍼블릭 IP 주소를 참조하세요.

인바운드 네트워크 보안 그룹 규칙 강화

무제한 액세스(Any 또는 `0.0.0.0/0`)를 허용하는 인바운드 네트워크 보안 그룹 규칙을 수정 또는 제거하고 워크로드에 필요한 특정 소스 범위, 포트 및 프로토콜에 대한 액세스를 제한합니다. 자세한 내용은 Microsoft Azure 설명서의 네트워크 보안 그룹을 참조하세요.

관리 액세스에 Azure Bastion 사용

관리 연결을 위해 Azure Bastion을 사용하여 퍼블릭 IP 주소 없이 TLS를 통해 가상 머신에 도달하거나 SSH/RDP 포트를 엽니다. 자세한 내용은 Microsoft Azure 설명서의 Azure Bastion을 참조하세요.

Azure 가상 머신의 취약성 특성

다음은 Azure 가상 머신의 취약성 특성과 제안된 문제 해결 단계입니다.

Azure 가상 머신에는 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있습니다.

일반적인 취약성 및 노출(CVEs)은 Azure 가상 머신에 설치된 소프트웨어 패키지에 영향을 미칠 수 있습니다. 우선순위가 높은 취약성은 네트워크 탐색이 가능하며 악용 가능성이 높습니다. 이는 공격자 또는 자동 스캔 도구가 익스플로잇 코드를 이미 공개적으로 사용할 수 있고 적극적으로 사용할 수 있기 때문에 즉각적인 보안 위협을 나타냅니다. 이러한 취약성을 즉시 패치하여 가상 머신을 보호합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

조사 결과 검토 및 수정

Microsoft Defender for Cloud 취약성 평가를 사용하여 영향을 받는 CVEs와 가상 머신의 수정 단계를 검토합니다. 각 조사 결과의 세부 정보 창에는 관련 CVEs와 권장 수정 사항이 포함되어 있습니다. 자세한 내용은 Microsoft Azure 설명서의 시스템 취약성 해결을 참조하세요.

업데이트 적용

Azure Update Manager를 사용하여 일정에 따라 가상 머신 전체에 운영 체제 및 소프트웨어 업데이트를 평가하고 배포합니다. 업데이트를 사용할 수 없는 경우 패치가 릴리스될 때까지 취약한 소프트웨어를 제거 또는 비활성화하거나 이에 대한 네트워크 액세스를 제한하는 것이 좋습니다. 자세한 내용은 Microsoft Azure 설명서의 Azure Update Manager를 참조하세요.

향후 고려 사항

향후 발생을 방지하려면 Microsoft Defender for Servers를 활성화하여 가상 머신에 취약성이 있는지 지속적으로 스캔하고 Azure Update Manager를 사용하여 정기적인 패치 적용 일정을 설정합니다. 자세한 내용은 Microsoft Azure 설명서의 서버용 Microsoft Defender를 참조하세요.

Azure 가상 머신에 소프트웨어 취약성이 있음

일반적인 취약성 및 노출(CVEs)은 Azure 가상 머신에 설치된 소프트웨어 패키지에 영향을 미칠 수 있습니다. 중요하지 않은 취약성은 우선순위가 높은 취약성보다 심각도 또는 악용 가능성이 낮은 보안 약점을 나타냅니다. 공격자는 덜 즉각적인 위험을 초래하지만 패치되지 않은 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습니다. 보안 모범 사례에 따라 이러한 취약성을 패치하여 가상 머신을 공격으로부터 보호합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

결과 검토 및 해결

Microsoft Defender for Cloud 취약성 평가를 사용하여 영향을 받는 CVEs를 검토하고 결과 세부 정보 창의 수정 단계를 따릅니다. 자세한 내용은 Microsoft Azure 설명서의 시스템 취약성 해결을 참조하세요.

업데이트 적용

Azure Update Manager를 사용하여 가상 머신 전체에 운영 체제 및 소프트웨어 업데이트를 평가하고 배포합니다. 대규모로 업데이트를 일관되게 관리하려면 예약된 패치 적용을 구성합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure Update Manager를 참조하세요.

Azure 가상 머신에 악성 소프트웨어 패키지가 있음

악성 패키지는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함된 소프트웨어 구성 요소입니다. 공격자는 별도의 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있으므로 악의적인 패키지는 가상 머신에 능동적이고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 패키지를 제거하여 잠재적 공격으로부터 가상 머신을 보호합니다.

문제 해결: 악성 패키지 조사 및 제거

조사 결과 세부 정보를 검토하여 위협을 이해하고 영향을 받는 패키지를 식별한 다음 운영 체제에 적합한 패키지 관리자를 사용하여 식별된 패키지를 제거합니다. 제거 후 스캔을 실행하여 관련된 악성 구성 요소가 남아 있지 않은지 확인합니다. 자세한 내용은 Microsoft Azure 설명서의 서버용 Microsoft Defender를 참조하세요.

## Azure Storage Blob 컨테이너에 대한 노출 문제 해결

AWS Security Hub는 Azure Storage Blob 컨테이너에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Azure Storage blob 컨테이너와 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 수정 지침에 따라 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure Storage Blob 컨테이너의 연결성 특성

  - 스토리지 계정은 익명 Blob 액세스를 허용합니다.
- Azure Storage Blob 컨테이너의 잘못된 구성 특성
  - 스토리지 계정은 전송 작업에 HTTPS가 필요하지 않습니다.
  - 스토리지 계정이 고객 관리형 키로 암호화되지 않음
  - 스토리지 계정은 테넌트 간 액세스를 허용합니다.
  - 스토리지 계정에 Blob 소프트 삭제가 비활성화되어 있습니다.
  - 스토리지 계정은 소프트 삭제된 BLOB의 영구 삭제를 허용합니다.
  - Azure Storage Blob 컨테이너에 Blob 버전 관리가 비활성화되었습니다.
  - 스토리지 컨테이너에 변경 불가능 정책이 없습니다.

Azure Storage Blob 컨테이너의 연결성 특성

다음은 Azure Storage Blob 컨테이너의 연결성 특성과 제안된 수정 단계입니다.

스토리지 계정은 익명 Blob 액세스를 허용합니다.

익명 읽기 액세스가 활성화된 경우 인증되지 않은 클라이언트는 권한 부여 없이 Blob 데이터를 읽을 수 있습니다. 스토리지 계정이 익명(퍼블릭) BLOB 액세스를 허용하고 컨테이너의 액세스 수준이 이를 허용하는 경우 퍼블릭 인터넷의 모든 사용자가 해당 컨테이너의 데이터를 읽을 수 있습니다. 표준 보안 원칙에 따라, 시나리오가 퍼블릭 읽기 액세스에 명시적으로 의존하지 않는 한 계정 수준에서 익명 액세스를 허용하지 않고 모든 요청을 승인해야 합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

스토리지 계정에 대한 익명 액세스 허용 안 함

스토리지 계정의 `AllowBlobPublicAccess` 속성을 로 설정합니다`false`. 계정 수준에서 익명 액세스를 허용하지 않으면 계정에 있는 모든 컨테이너의 액세스 설정이 재정의되고 향후 익명 요청이 차단됩니다. 자세한 내용은 Microsoft Azure 설명서의 익명 읽기 액세스 방지를 참조하세요.

컨테이너 액세스 수준을 프라이빗으로 설정

퍼블릭 액세스를 위해 개별 컨테이너가 구성된 경우 모든 요청에 승인이 필요`Private`하도록 각 컨테이너의 익명 액세스 수준을 로 설정합니다. 설정을 변경하기 전에 익명 액세스에 의존할 수 있는 클라이언트 애플리케이션을 검토합니다. 자세한 내용은 Microsoft Azure 설명서의 익명 읽기 액세스 구성을 참조하세요.

Azure Storage Blob 컨테이너의 잘못된 구성 특성

다음은 Azure Storage Blob 컨테이너의 잘못된 구성 특성과 제안된 수정 단계입니다.

스토리지 계정은 전송 작업에 HTTPS가 필요하지 않습니다.

스토리지 계정에 보안 전송이 필요하지 않은 경우 암호화되지 않은 HTTP를 통한 요청을 수락합니다. HTTP를 통해 전송된 데이터 및 자격 증명은 네트워크 경로의 공격자가 전송 중에 가로채거나 수정할 수 있습니다. 표준 보안 원칙에 따라 계정이 HTTPS를 통해서만 요청을 수락하도록 보안 전송이 필요합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

보안 전송 필요

스토리지 계정( 속성)에서 보안 전송 필수 `enableHttpsTrafficOnly` 속성을 활성화합니다. 보안 전송이 필요한 경우 HTTP를 통한 모든 요청이 거부됩니다. 자세한 내용은 Microsoft Azure 설명서의 보안 전송 요구 섹션을 참조하세요.

최소 TLS 버전 적용

이전 버전의 덜 안전한 프로토콜 버전을 사용하는 요청이 거부되도록 스토리지 계정의 최소 TLS 버전을 1.2( `minimumTlsVersion` 속성)로 설정합니다. 이 설정을 적용하기 전에 클라이언트가 TLS 1.2를 지원하는지 확인합니다. 자세한 내용은 Microsoft Azure 설명서의 스토리지 계정의 최소 TLS 버전 구성을 참조하세요.

스토리지 계정이 고객 관리형 키로 암호화되지 않음

기본적으로 Azure Storage는 Microsoft 관리형 키를 사용하여 저장 데이터를 암호화합니다. 고객 관리형 키(CMK)를 사용하면 키에 대한 액세스 권한을 교체, 취소 및 감사하는 기능을 포함하여 데이터를 보호하는 키를 제어할 수 있습니다. 조직의 규정 준수 요구 사항에서 암호화 키에 대한 제어를 요구하는 경우 고객 관리형 키의 부재는 격차입니다. 데이터 보호 모범 사례에 따라 Azure Key Vault 또는 관리형 HSM에 저장된 고객 관리형 키를 사용하도록 스토리지 계정을 구성합니다.

문제 해결: 고객 관리형 키 구성

소프트 삭제 및 제거 보호가 활성화된 상태에서 Azure Key Vault 또는 Azure Key Vault 관리형 HSM에 키를 저장합니다. 관리형 자격 증명에 `get`, `wrapkey`및 `unwrapkey` 권한을 부여한 다음 암호화에 해당 키를 사용하도록 스토리지 계정을 구성합니다. 언제든지 고객 관리형 키와 Microsoft 관리형 키 간에 전환할 수 있습니다. 자세한 내용은 Microsoft Azure 설명서의 스토리지 암호화를 위한 고객 관리형 키를 참조하세요.

스토리지 계정은 테넌트 간 액세스를 허용합니다.

교차 테넌트 객체 복제 또는 교차 테넌트 공유 액세스 서명(SAS) 위임과 같은 교차 테넌트 액세스 설정으로 인해 데이터가 스토리지 계정을 소유한 Microsoft Entra 테넌트를 떠날 수 있습니다. 워크로드에서 테넌트 간에 데이터를 공유할 필요가 없는 경우 이러한 설정을 활성화하면 데이터가 테넌트 경계를 벗어날 위험이 높아집니다. 표준 보안 원칙에 따라 명시적으로 필요하지 않은 한 교차 테넌트 액세스를 비활성화합니다.

문제 해결: 테넌트 간 액세스 설정 비활성화

스토리지 계정에서 교차 테넌트 객체 복제를 비활성화하고(`allowCrossTenantReplication`로 설정`false`) 지원되는 경우 교차 테넌트 SAS 위임을 제한합니다. 변경하기 전에 복제 및 공유 요구 사항을 검토합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure Storage 계정 개요를 참조하세요.

스토리지 계정에 Blob 소프트 삭제가 비활성화되어 있습니다.

블롭 소프트 삭제는 우발적이거나 악의적인 삭제 및 덮어쓰기로부터 개별 블롭, 스냅샷 및 버전을 보호합니다. 삭제된 데이터는 사용자가 복원할 수 있는 구성 가능한 보존 기간 동안 보존됩니다. 소프트 삭제가 비활성화되면 삭제되거나 덮어쓴 BLOB 데이터를 복구할 수 없으므로 계정이 영구적으로 손실됩니다. 데이터 보호 모범 사례에 따라 적절한 보존 기간으로 BLOB 소프트 삭제를 활성화합니다.

문제 해결: Blob 소프트 삭제 활성화

스토리지 계정에서 Blob 소프트 삭제를 활성화하고 복구 요구 사항을 충족하는 보존 기간(1~365일)을 설정합니다. 보다 완벽한 보호를 위해 컨테이너 소프트 삭제 및 Blob 버전 관리를 활성화합니다. 자세한 내용은 Microsoft Azure 설명서의 Blob에 대한 소프트 삭제를 참조하세요.

스토리지 계정은 소프트 삭제된 BLOB의 영구 삭제를 허용합니다.

영구 삭제가 허용되면( `allowPermanentDelete` 속성은 `true`) 소프트 삭제 보존 기간이 만료되기 전에 소프트 삭제 블롭과 스냅샷을 제거할 수 있습니다. 이렇게 하면 사용자 또는 손상된 보안 주체가 보존 기간이 만료되기 전에 복구 가능한 데이터를 영구적으로 삭제할 수 있으므로 소프트 삭제가 제공하는 보호 기능이 약화됩니다. 데이터 보호 모범 사례에 따라 구체적이고 잘 이해된 요구 사항이 없는 한 소프트 삭제된 BLOB의 영구 삭제를 허용하지 마세요.

해결 방법: 영구 삭제 비활성화

소프트 삭제된 BLOB 및 스냅샷이 전체 보존 기간 동안 복구 가능한 상태로 유지`false`되도록 스토리지 계정의 `allowPermanentDelete` 속성을 로 설정합니다. 자세한 내용은 Microsoft Azure 설명서의 Blob에 대한 소프트 삭제를 참조하세요.

Azure Storage Blob 컨테이너에 Blob 버전 관리가 비활성화되었습니다.

Blob 버전 관리는 이전 버전의 Blob을 자동으로 유지합니다. Blob을 수정하거나 삭제하면 이전 상태가 복원할 수 있는 이전 버전으로 유지됩니다. 버전 관리를 비활성화하면 덮어쓰기 및 삭제를 이전 상태로 롤백할 수 없으므로 복구할 수 없는 데이터 손실 또는 손상 위험이 증가합니다. 데이터 보호 모범 사례에 따라 최적의 데이터 보호를 위해 소프트 삭제와 함께 Blob 버전 관리를 활성화합니다.

문제 해결: Blob 버전 관리 활성화

스토리지 계정의 Blob 서비스에서 버전 관리를 활성화합니다. 여러 버전을 유지하는 데 드는 비용을 제어하려면 수명 주기 관리 정책을 사용하여 이전 버전을 자동으로 삭제합니다. 자세한 내용은 Microsoft Azure 설명서의 Blob 버전 관리를 참조하세요.

스토리지 컨테이너에 변경 불가능 정책이 없습니다.

불변성 정책은 BLOB 데이터를 WORM(Write Once, Read Many) 상태로 저장합니다. 이 상태에서는 지정된 간격(시간 기반 보존 정책) 동안 또는 법적 보존이 지워질 때까지 데이터를 수정하거나 삭제할 수 없습니다. 불변성 정책이 없으면 권한이 있는 사용자를 포함하여 컨테이너의 비즈니스 크리티컬 또는 규정 준수 관련 데이터를 덮어쓰거나 삭제할 수 있습니다. 규제 또는 데이터 무결성 요구 사항이 적용되는 경우 컨테이너에 대한 불변성 정책을 구성합니다.

문제 해결: 불변성 정책 구성

컨테이너에 대한 시간 기반 보존 정책 또는 법적 보존을 구성합니다. 테스트가 완료되면 시간 기반 정책을 잠가서 데이터가 WORM 상태로 완전히 보호되도록 합니다. 추가 보호를 위해 불변성 정책을 적용하기 전에 소프트 삭제를 활성화합니다. 자세한 내용은 Microsoft Azure 설명서의 Blob 데이터에 대한 변경 불가능한 스토리지를 참조하세요.

## Azure SQL 데이터베이스의 노출 문제 해결

AWS Security Hub는 Azure SQL 데이터베이스에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서는 노출 조사 결과와 관련된 Azure SQL 데이터베이스와 해당 식별 정보가 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 문제 해결 지침은 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure SQL 데이터베이스의 잘못된 구성 특성
  - Azure SQL 데이터베이스에 퍼블릭 네트워크 액세스가 활성화되어 있음
  - Azure SQL 데이터베이스는 Azure AD 전용 인증을 적용하지 않습니다.
  - Azure SQL 데이터베이스는 기본 또는 공통 관리자 사용자 이름을 사용합니다.
  - Azure SQL 데이터베이스에 지리 중복 백업이 비활성화되어 있음


## Azure SQL 데이터베이스의 잘못된 구성 특성

다음은 Azure SQL 데이터베이스의 잘못된 구성 특성과 제안된 수정 단계입니다.

### Azure SQL 데이터베이스에 퍼블릭 네트워크 액세스가 활성화되어 있음

논리적 서버에서 퍼블릭 네트워크 액세스가 활성화되면 퍼블릭 엔드포인트를 통해 데이터베이스에 연결할 수 있으며 퍼블릭 인터넷에서 연결을 수락할 수 있습니다(방화벽 규칙 적용). 퍼블릭 엔드포인트는 데이터베이스의 공격 표면을 늘리고 무단 연결 시도에 노출합니다. 표준 보안 원칙에 따라 퍼블릭 네트워크 액세스를 비활성화하고 데이터베이스에 비공개로 연결하거나 서버 방화벽 규칙을 엄격하게 제한합니다.

#### 문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

#### 퍼블릭 네트워크 액세스 비활성화 및 프라이빗 링크 사용

에 대한 논리적 서버의 퍼블릭 네트워크 액세스를 설정하고 가상 네트워크 내의 프라이빗 엔드포인트(Azure Private Link)를 통해 데이터베이스에 `Disabled` 연결합니다. 이렇게 하면 Azure 백본과 퍼블릭 인터넷에서 데이터베이스 트래픽이 유지됩니다. 자세한 내용은 Microsoft Azure 설명서의 Azure SQL Database에 대한 네트워크 액세스 제어를 참조하세요.

퍼블릭 액세스가 필요한 경우 방화벽 규칙 제한

퍼블릭 액세스를 활성화해야 하는 경우 전체 인터넷 범위를 허용하는 규칙을 제거하고 필요하지 않은 경우 Azure 서비스 및 리소스가이 서버에 액세스하도록 허용을 비활성화합니다. 서버 수준 방화벽 규칙을 워크로드에 필요한 신뢰할 수 있는 특정 IP 주소로 제한합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure SQL Database에 대한 네트워크 액세스 제어를 참조하세요.

최소 TLS 버전 적용

이전 버전의 덜 안전한 프로토콜 버전을 사용하는 연결이 거부되도록 논리적 서버의 최소 TLS 버전을 1.2로 설정합니다. 이 설정을 적용하기 전에 클라이언트가 TLS 1.2를 지원하는지 확인합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure SQL Database에 대한 연결 설정을 참조하세요.

Azure SQL 데이터베이스는 Azure AD 전용 인증을 적용하지 않습니다.

Microsoft Entra 전용 인증(이전 Azure AD 전용 인증)이 적용되지 않는 경우 논리적 서버는 데이터베이스 내에 저장되고 관리되는 암호에 의존하는 SQL 인증도 수락합니다. SQL 인증은 자격 증명 도용 및 무차별 대입 공격에 더 취약하며 조건부 액세스 및 멀티 팩터 인증과 같은 중앙 집중식 Microsoft Entra 제어의 이점을 얻지 못합니다. 표준 보안 원칙에 따라 Microsoft Entra 자격 증명만 연결할 수 있도록 Microsoft Entra 전용 인증을 적용합니다.

문제 해결: Microsoft Entra 전용 인증 적용

논리적 서버에 대한 Microsoft Entra 관리자를 설정한 다음 Microsoft Entra 전용 인증을 활성화합니다. 이렇게 하면 Microsoft Entra 자격 증명만 서버 및 데이터베이스에 연결할 수 있도록 SQL 인증이 비활성화됩니다. 이 설정을 적용하기 전에 애플리케이션이 Microsoft Entra 인증을 지원하는지 확인합니다. 자세한 내용은 Microsoft Azure 설명서의 Microsoft Entra 전용 인증을 참조하세요.

Azure SQL 데이터베이스는 기본 또는 공통 관리자 사용자 이름을 사용합니다.

논리적 서버의 관리자 로그인은 , 또는와 같이 잘 알려져 있거나 일반적인 사용자 이름을 사용합니다`sqladminadminsa`. 일반적인 관리자 사용자 이름을 예측할 수 있으므로 공격자가 암호만 추측하면 되므로 서버가 무차별 대입 공격 및 자격 증명 스터핑 공격의 대상이 더 쉬워집니다. 표준 보안 원칙에 따라 기본 또는 일반 관리자 사용자 이름을 피하고 Microsoft Entra ID를 통해 관리 액세스를 중앙 집중화합니다.

문제 해결: 기본이 아닌 관리자 및 Microsoft Entra 인증 사용

예측 가능한 관리자 로그인 이름을 사용하지 마세요. 가능하면 Microsoft Entra 전용 인증을 적용하고 SQL 관리자 로그인 대신 Microsoft Entra 자격 증명 및 그룹을 통해 관리 액세스를 관리합니다. 로그인

및 최소 권한 액세스를 관리하기 위한 Azure SQL 보안 모범 사례를 따릅니다. 자세한 내용은 Microsoft Azure 설명서의 Azure SQL 데이터베이스 보안 모범 사례를 참조하세요.

Azure SQL 데이터베이스에 지리 중복 백업이 비활성화되어 있음

Azure SQL Database는 기본적으로 지리 중복 스토리지에 자동 백업을 저장합니다.이 스토리지는 백업을 페어링된 리전에 복제하고 리전 중단 시 지리 복원을 활성화합니다. 백업 스토리지 중복이 로컬 중복 또는 영역 중복 스토리지로 설정된 경우 지리 복원을 사용할 수 없습니다. 기본 리전을 사용할 수 없게 되면 다른 리전에서 데이터베이스를 복구할 수 없습니다. 데이터 보호 모범 사례에 따라 리전 중단에 대한 복원력이 필요한 데이터베이스에는 지리 중복 백업 스토리지를 사용합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

지리 중복 백업 스토리지 구성

지리 복원을 사용할 수 있도록 데이터베이스의 백업 스토리지 중복을 지리 중복 스토리지(GRS) 또는 geo-zone-redundant 스토리지(GZRS)로 설정합니다. 변경 사항은 향후 백업에 적용되며 적용되는 데 최대 48시간이 걸릴 수 있습니다. 자세한 내용은 Microsoft Azure 설명서의 Azure SQL 데이터베이스의 자동 백업을 참조하세요.

장기 보존 구성

규정 준수 또는 장기 복구 요구 사항이 있는 데이터베이스의 경우 장기 보존(LTR) 정책을 구성합니다. LTR은 기본 단기 보존 외에도 최대 10년 동안 전체 백업을 보존합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure SQL 데이터베이스의 장기 보존을 참조하세요.

## Azure Cosmos DB 계정에 대한 노출 문제 해결

AWS Security Hub는 Azure Cosmos DB 계정에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Azure Cosmos DB 계정과 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 수정 지침에 따라 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure Cosmos DB 계정에 대한 잘못된 구성 특성
  - Azure Cosmos DB 계정에 퍼블릭 네트워크 액세스가 활성화되어 있습니다.
  - Azure Cosmos DB 계정은 연속 백업을 사용하지 않습니다.


## Azure Cosmos DB 계정에 대한 잘못된 구성 특성

다음은 Azure Cosmos DB 계정의 잘못된 구성 특성과 제안된 수정 단계입니다.

### Azure Cosmos DB 계정에 퍼블릭 네트워크 액세스가 활성화되어 있습니다.

퍼블릭 네트워크 액세스가 활성화되면 퍼블릭 엔드포인트를 통해 Azure Cosmos DB 계정에 연결할 수 있습니다. 방화벽 및 가상 네트워크 규칙에 따라 퍼블릭 인터넷의 연결을 수락할 수 있습니다. 퍼블릭 엔드포인트는 계정의 공격 표면을 늘리고 무단 연결 시도 및 잠재적 데이터 유출에 노출합니다. 표준 보안 원칙에 따라 퍼블릭 네트워크 액세스를 비활성화하고 계정에 비공개로 연결하거나 계정 방화벽 규칙을 엄격하게 제한합니다.

#### 문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

#### 퍼블릭 네트워크 액세스 비활성화 및 프라이빗 링크 사용

계정의 `publicNetworkAccess` 속성을 `Disabled` 로 설정하고 가상 네트워크 내의 프라이빗 엔드포인트(Azure Private Link)를 통해 연결합니다. 제한적인 네트워크 보안 그룹 정책과 결합하면 프라이빗 엔드포인트가 데이터 유출 위험을 줄이는 데 도움이 됩니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 프라이빗 링크 구성을 참조하세요.

#### 퍼블릭 액세스가 필요한 경우 방화벽 규칙 제한

퍼블릭 액세스를 활성화해야 하는 경우 모든 네트워크를 허용하는 대신 워크로드에 필요한 신뢰할 수 있는 특정 소스만 허용하도록 IP 방화벽 규칙과 가상 네트워크 규칙을 구성합니다. 자세한 내용은 Microsoft Azure 설명서의 IP 방화벽 구성을 참조하세요.

Azure Cosmos DB 계정은 연속 백업을 사용하지 않습니다.

연속 백업 모드를 사용하면 point-in-time으로 복원을 사용하여 우발적인 쓰기 또는 삭제로부터 복구할 수 있습니다. 또한 삭제된 데이터베이스 또는 컨테이너를 보존 기간 내의 모든 타임스탬프로 복원할 수 있습니다. 계정이 연속 백업 대신 주기적 백업 모드를 사용하는 경우 셀프 서비스 point-in-time 수행할 수 없습니다. 이 제한은 우발적이거나 악의적인 변경 후 복구 시간과 데이터 손실 위험을 높입니다. 데이터 보호 모범 사례에 따라 워크로드가 지원하는 연속 백업 모드를 활성화합니다.

문제 해결: 연속 백업 모드 활성화

point-in-time으로 복원을 사용할 수 있도록 연속 백업 모드(7일 또는 30일 계층)를 사용하도록 계정을 구성합니다. 정기 백업에서 연속 백업으로 마이그레이션하기 전에 현재 제한 사항과 지원되는 APIs를 검토합니다. 자세한 내용은 Microsoft Azure 설명서의 point-in-time 복원을 사용한 연속 백업을 참조하세요.

## Azure Function 앱의 노출 문제 해결

AWS Security Hub는 Azure Function 앱에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Azure Function 앱과 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 수정 지침에 따라 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure Function 앱의 잘못된 구성 특성
  - Azure Function 앱이 VNet 외부에 배포됩니다.
  - Azure Function 앱과 연결된 역할에는 관리 액세스 역할 할당이 있습니다.
- Azure Function 앱의 연결성 특성
  - Azure Function 앱은 익명 HTTP 트리거 호출을 허용합니다.
- Azure Function 앱의 취약성 특성
  - Azure Function 앱에는 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있습니다.
  - Azure Function 앱에 소프트웨어 취약성이 있음
  - Azure Function 앱에 악성 소프트웨어 패키지가 있음


## Azure Function 앱의 잘못된 구성 특성

다음은 Azure Function 앱의 잘못된 구성 특성과 제안된 수정 단계입니다.

### Azure Function 앱이 VNet 외부에 배포됩니다.

함수 앱이 가상 네트워크와 통합되지 않은 경우 해당 엔드포인트와 아웃바운드 트래픽은 프라이빗 네트워크 경계가 아닌 퍼블릭 네트워크를 통과합니다. 함수 앱이 가상 네트워크와 통합되지 않은 경우 프라이빗 엔드포인트, 네트워크 보안 그룹 및 제한된 아웃바운드 액세스와 같은 네트워크 수준 제어를 적용할 수 없습니다. 이 간격은 앱의 노출을 증가시킵니다. 표준 보안 원칙에 따라 함수 앱을 가상 네트워크와 통합하고 호스팅 계획이 지원하는 프라이빗 엔드포인트를 사용합니다.

#### 문제 해결

이 노출을 해결하려면 다음 작업 중 하나 이상을 수행합니다.

##### 함수 앱을 가상 네트워크와 통합

함수 앱에 대해 가상 네트워크 통합을 활성화합니다. 호스팅 플랜(플렉스 소비, Elastic Premium 또는 전용)에서 지원하는 경우 프라이빗 엔드포인트를 사용하여 네트워크 내에서만 앱에 연결할 수 있습니다. 자세한 내용은 Microsoft Azure 설명서의 Azure Functions 네트워킹 옵션을 참조하세요.

##### 인바운드 액세스 제한

프라이빗 엔드포인트를 지원하지 않는 호스팅 계획에서는 액세스 제한을 사용하여 신뢰할 수 있는 IP 주소 범위의 인바운드 트래픽만 허용하고 필요하지 않은 퍼블릭 네트워크 액세스를 비활성화합니다. 자세한 내용은 Microsoft Azure 설명서의 액세스 제한 설정을 참조하세요.

Azure Function 앱과 연결된 역할에는 관리 액세스 역할 할당이 있습니다.

Azure Function 앱에 관리형 자격 증명을 할당하고 다른 Azure 리소스에 액세스할 수 있도록 Azure 역할 기반 액세스 제어(Azure RBAC) 역할 할당을 부여할 수 있습니다. 연결된 자격 증명에 광범위한 범위의 관리 역할 할당(예: `Owner` 또는 `Contributor`)이 있는 경우 일반적으로 앱에 필요한 것 이상의 권한을 부여합니다. 함수 앱이 손상된 경우 공격자는 이러한 과도한 권한을 사용하여 환경 전체에서 내부적으로 이동하거나, 데이터에 액세스하거나, 리소스를 조작할 수 있습니다. 표준 보안 원칙에 따라 앱에 필요한 권한만 할당하여 최소 권한을 부여합니다.

문제 해결

이 노출을 해결하려면 다음 작업 중 하나 이상을 수행합니다.

관리 역할 할당 검토 및 식별

Azure 포털에서 함수 앱과 연결된 자격 증명에 대한 역할 할당을 검토합니다. `Owner`에서 와일드카드(*)를 사용하는 사용자 지정 역할에 대해 `User Access Administrator`, `Contributor`또는와 같은 권한이 있는 관리자 역할을 찾습니다`Actions`. 자세한 내용은 Microsoft Azure 설명서의 Azure 역할 할당 나열을 참조하세요.

최소 권한 액세스 구현

관리 역할 할당을 앱에 필요한 권한만 부여하는 최소 권한의 기본 제공 역할로 바꾸고 필요에 맞는 가장 좁은 범위에 할당합니다. 다른 Azure 서비스에 연결하기 위해 저장된 보안 암호 대신 관리형 자격 증명을 사용합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure RBAC 모범 사례를 참조하세요.

Azure Function 앱의 연결성 특성

다음은 Azure Function 앱의 연결성 특성과 제안된 문제 해결 단계입니다.

Azure Function 앱은 익명 HTTP 트리거 호출을 허용합니다.

권한 부여 수준이 로 설정된 HTTP 트리거 함수는 액세스 키나 인증 없이 인터넷을 통해 호출할 `anonymous` 수 있습니다. 익명 HTTP 트리거는 인증되지 않은 호출자에게 함수 로직을 노출하므로 제어되지 않은 호출을 통해 남용, 데이터 노출 또는 denial-of-wallet가 발생할 수 있습니다. 익명 액세스가 명시적으로 필요하지 않은 한 표준 보안 원칙에 따라 HTTP 트리거 함수에 대한 인증 또는 액세스 키가 필요합니다.

문제 해결

이 노출을 해결하려면 다음 작업 중 하나 이상을 수행합니다.

HTTP 트리거에 대한 권한 부여 필요

요청에 유효한 액세스 키가 포함되고 HTTPS가 필요`admin`하도록 HTTP 트리거 권한 부여 수준을 `anonymous`에서 `function` 또는 로 높입니다. 더 강력한 보호를 위해 앱 서비스 인증/권한 부여를 활성화하거나 Azure API Management를 사용하여 앱을 앞에 배치합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 함수 보호를 참조하세요.

관리형 자격 증명 공급자를 통한 인증 필요

액세스 키는 인증이 아닌 권한 부여 제어이므로 호출자가 유효한 자격 증명을 제시해야 하도록 Microsoft Entra ID를 사용하여 앱 서비스 인증(Easy Auth)을 활성화합니다. 또한 필요하지 않은 경우 관리 엔드포인트(`/admin`라우팅)를 비활성화합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 함수 보호를 참조하세요.

Azure Function 앱의 취약성 특성

다음은 Azure Function 앱의 취약성 특성과 제안된 문제 해결 단계입니다.

Azure Function 앱에는 악용 가능성이 높은 네트워크 탐색 가능 소프트웨어 취약성이 있습니다.

일반적인 취약성 및 노출(CVEs)은 함수 앱의 소프트웨어 패키지 및 종속성에 영향을 미칠 수 있습니다. 우선 순위가 높은 취약성은 공격자가 이미 공개적으로 사용할 수 있고 적극적으로 사용할 수 있기 때문에 즉각적인 보안 위협을 나타내는 악용 가능성이 높은 네트워크 배포 가능 취약성입니다. 이러한 취약성을 즉시 패치하여 함수 앱을 보호합니다.

문제 해결

이 노출을 해결하려면 다음 작업 중 하나 이상을 수행합니다.

영향을 받는 종속성 업데이트

조사 결과에서 영향을 받는 CVEs를 검토한 다음 취약한 패키지와 종속성을 최신 보안 버전으로 업데이트하고 앱을 재배포합니다. 플랫폼 보안 업데이트가 계속 적용되도록 함수 앱을 지원되는 런타임에 유지합니다. 자세한 내용은 Microsoft Azure 설명서의 Microsoft Defender for App Service를 참조하세요.

향후 고려 사항

향후 발생을 방지하려면 종속성 및 취약성 스캔을 빌드 및 배포 파이프라인에 통합하고 Microsoft Defender for Cloud를 사용하여 앱의 구성 및 취약성 조사 결과를 모니터링합니다. 자세한 내용은 Microsoft Azure 설명서의 Microsoft Defender for App Service를 참조하세요.

Azure Function 앱에 소프트웨어 취약성이 있음

일반적인 취약성 및 노출(CVEs)은 함수 앱의 소프트웨어 패키지 및 종속성에 영향을 미칠 수 있습니다. 중요하지 않은 취약성은 우선순위가 높은 취약성보다 심각도 또는 악용 가능성이 낮은 보안 약점을 나타냅니다. 공격자는 덜 즉각적인 위험을 초래하지만 패치되지 않은 취약성을 악용하여 데이터의 기밀성, 무결성 또는 가용성을 손상시키거나 다른 시스템에 액세스할 수 있습니다. 보안 모범 사례에 따라 이러한 취약성을 패치하여 함수 앱을 보호합니다.

문제 해결: 영향을 받는 종속성 업데이트

취약한 패키지와 종속성을 최신 보안 버전으로 업데이트하고 앱을 재배포합니다. 업데이트를 사용할 수 없는 경우 패치가 릴리스될 때까지 취약한 구성 요소를 제거하거나 비활성화하는 것이 좋습니다. 자세한 내용은 Microsoft Azure 설명서의 Microsoft Defender for App Service를 참조하세요.

Azure Function 앱에 악성 소프트웨어 패키지가 있음

악성 패키지는 시스템 및 데이터의 기밀성, 무결성 및 가용성을 손상시키도록 설계된 유해한 코드가 포함된 소프트웨어 구성 요소입니다. 공격자는 별도의 취약성을 악용하지 않고 악성 코드를 자동으로 실행할 수 있으므로 악성 패키지는 함수 앱에 능동적이고 중요한 위협을 가합니다. 보안 모범 사례에 따라 악성 패키지를 제거하여 잠재적 공격으로부터 Function 앱을 보호합니다.

문제 해결: 악성 패키지 조사 및 제거

결과 세부 정보를 검토하여 영향을 받는 패키지를 식별하고, 프로젝트 종속성에서 제거하며, 신뢰할 수 있는 소스에서 다시 빌드하고, 앱을 재배포합니다. 문제 해결 후 종속성 공급망을 감사하여 관련된 악성 구성 요소가 남아 있지 않은지 확인합니다. 자세한 내용은 Microsoft Azure 설명서의 Microsoft Defender for App Service를 참조하세요.

## Azure Container 앱의 노출 문제 해결

AWS Security Hub는 Azure Container 앱에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Azure 컨테이너 앱과 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 수정 지침에 따라 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure Container 앱의 잘못된 구성 특성
  - Azure Container 앱의 환경 변수에 일반 텍스트 자격 증명이 있음
  - Azure Container 앱에는 개방형 네트워크 보안 그룹이 있습니다.
  - Azure Container 앱에는 최소 권한을 따르지 않는 관리형 자격 증명이 있습니다.
  - Azure Container 앱과 연결된 역할에는 관리 액세스 역할 할당이 있습니다.
- Azure Container 앱의 연결성 특성
  - Azure Container 앱은 인터넷을 통해 연결할 수 있습니다.


## Azure Container 앱의 잘못된 구성 특성

다음은 Azure Container 앱의 잘못된 구성 특성과 제안된 수정 단계입니다.

### Azure Container 앱의 환경 변수에 일반 텍스트 자격 증명이 있음

컨테이너 앱은 연결 문자열, API 키 또는 암호와 같은 보안 암호 데이터를 컨테이너에 일반 텍스트 환경 변수로 전달합니다. 구성, 로그 또는 손상된 컨테이너는 환경 변수에 일반 텍스트 자격 증명을 노출하여 공격자가 이를 재사용하여 다른 시스템에 액세스할 수 있습니다. 표준 보안 원칙에 따라 민감한 값을 일반 텍스트로 임베딩하지 않고 보안 암호로 저장하고 참조합니다.

#### 문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

#### 보안 인증 정보를 보안 암호로 이동

일반 텍스트 환경 변수 값을 컨테이너 앱 보안 암호로 바꾸거나 Azure Key Vault에 저장된 보안 암호를 참조합니다. 컨테이너를 업데이트하여 해당 보안 암호 참조의 값을 읽습니다. 이전에 일반 텍스트로 노

출된 자격 증명을 교체합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 컨테이너 앱에서 보안 암호 관리를 참조하세요.

가능한 경우 관리형 자격 증명 사용

Azure 서비스에 연결하는 경우 보안 암호를 전혀 저장하지 않고 컨테이너 앱의 관리형 자격 증명을 사용합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 컨테이너 앱의 관리형 자격 증명을 참조하세요.

Azure Container 앱에는 개방형 네트워크 보안 그룹이 있습니다.

컨테이너 앱의 환경을 보호하는 네트워크 보안 그룹에는 모든 소스(예: Any 또는 소스)에서 무제한 액세스를 허용하는 규칙이 포함되어 있습니다`0.0.0.0/0`. 개방형 네트워크 보안 그룹은 컨테이너 앱의 환경을 인터넷에서 무단 액세스에 노출합니다. 표준 보안 원칙에 따라 네트워크 보안 그룹 규칙을 워크로드에 필요한 특정 IP 주소, 포트 및 프로토콜로만 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

네트워크 보안 그룹 규칙 제한

컨테이너 앱 환경의 서브넷과 연결된 네트워크 보안 그룹을 검토하고 무제한 액세스를 허용하는 규칙을 수정하거나 제거합니다. 와 같은 광범위한 소스를 워크로드에 필요한 신뢰할 수 있는 특정 범위Any로 바꿉니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 컨테이너 앱의 네트워킹을 참조하세요.

IP 수신 제한 설정

환경 서브넷의 네트워크 보안 그룹 규칙 외에도 IP 주소 범위별로 인바운드 트래픽을 허용하거나 거부하도록 컨테이너 앱 자체에 대한 IP 수신 제한을 구성합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 컨테이너 앱에서 IP 수신 제한 설정을 참조하세요.

Azure Container 앱에는 최소 권한을 따르지 않는 관리형 자격 증명이 있습니다.

컨테이너 앱에는 워크로드에 필요한 것보다 더 많은 액세스 권한이 부여된 관리형 자격 증명이 있습니다. 공격자가 자격 증명의 모든 권한으로 작업할 수 있으므로 과권 관리형 자격 증명은 컨테이너 앱이 손상된 경우 폭발 반경을 넓힙니다. 표준 보안 원칙에 따라 가장 좁은 범위에서 워크로드에 필요한 권한만 자격 증명에 부여합니다.

문제 해결: 관리형 자격 증명의 범위를 최소 권한으로 지정합니다.

컨테이너 앱의 관리형 자격 증명에 부여된 역할 할당을 검토하고 필요하지 않은 모든를 제거합니다. 필요에 맞는 가장 좁은 범위(리소스 또는 리소스 그룹)에서 최소 권한의 내장 역할을 할당합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure RBAC 모범 사례를 참조하세요.

Azure Container 앱과 연결된 역할에는 관리 액세스 역할 할당이 있습니다.

컨테이너 앱과 연결된 관리형 자격 증명에는 광범위한 관리 역할 할당(예: `Owner` 또는 `Contributor`)이 있습니다. 이 할당은 일반적으로 워크로드에 필요한 것 이상의 권한을 부여합니다. 컨테이너 앱이 손상된 경우 공격자는 이러한 과도한 권한을 사용하여 환경 전체에서 내부적으로 이동하거나, 데이터에 액세스하거나, 리소스를 조작할 수 있습니다. 표준 보안 원칙에 따라 앱에 필요한 권한만 할당하여 최소 권한을 부여합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

관리 역할 할당 검토 및 식별

Azure 포털에서 컨테이너 앱과 연결된 자격 증명에 대한 역할 할당을 검토합니다. `Owner`에서 와일드카드(*)를 사용하는 사용자 지정 역할에 대해 `User Access Administrator`, `Contributor`또는와 같은 권한이 있는 관리자 역할을 찾습니다`Actions`. 자세한 내용은 Microsoft Azure 설명서의 Azure 역할 할당 나열을 참조하세요.

최소 권한 액세스 구현

관리 역할 할당을 앱에 필요한 권한만 부여하는 최소 권한의 기본 제공 역할로 바꾸고 필요에 맞는 가장 좁은 범위에서 할당합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure RBAC 모범 사례를 참조하세요.

Azure Container 앱의 연결성 특성

다음은 Azure Container 앱의 연결성 특성과 제안된 문제 해결 단계입니다.

Azure Container 앱은 인터넷을 통해 연결할 수 있습니다.

외부 수신이 활성화되었거나(`ingress.external`가 로 설정됨`true`) 환경에 퍼블릭 IP 주소가 있기 때문에 퍼블릭 인터넷에서 컨테이너 앱에 연결할 수 있습니다. 퍼블릭 연결성은 컨테이너 앱의 공격 표면을 증가시키고 무단 요청에 노출합니다. 표준 보안 원칙에 따라 필요하지 않은 외부 수신을 비활성화하거나, 내부 환경을 사용하거나, 앱을 제어되고 인증된 수신 지점 뒤에 배치합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

외부 수신 제한 또는 제거

가상 네트워크 또는 환경 내에서만 앱에 연결해야 하는 경우 수신을 내부로 설정합니다. 퍼블릭 액세스가 필요한 경우 수신 IP 제한으로 제한합니다. Azure Application Gateway 또는 Azure Front Door와 같은 게이트웨이를 사용하여 앱을 앞당깁니다.

이러한 게이트웨이는 인증 및 웹 애플리케이션 방화벽을 제공합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 컨테이너 앱의 수신을 참조하세요.

내부 환경 사용

퍼블릭 IP 주소 할당을 방지하려면 프라이빗 IP 주소를 사용하는 내부(가상 네트워크 통합) 환경에 컨테이너 앱을 배포하고 제어된 수신 지점을 통해 퍼블릭이어야 하는 엔드포인트만 노출합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 컨테이너 앱의 네트워킹을 참조하세요.

퍼블릭 수신을 위해 HTTPS 및 인증 필요

수신이 퍼블릭으로 유지되어야 하는 경우 트래픽이 HTTPS를 통해서만 제공되도록 안전하지 않은 연결(`allowInsecure`로 설정`false`)을 비활성화합니다. 인증되지 않은 요청이 거부되도록 Microsoft Entra ID로 기본 제공 인증 기능을 활성화합니다. 자세한 내용은 Microsoft Azure 설명서의 Azure 컨테이너 앱의 인증 및 권한 부여를 참조하세요.

## Azure Kubernetes Service 클러스터에 대한 노출 문제 해결

AWS Security Hub는 Azure Kubernetes Service(AKS) 클러스터에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 AKS 클러스터와 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 수정 지침에 따라 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure Kubernetes Service 클러스터의 잘못된 구성 특성
  - Azure Kubernetes Service 클러스터가 지원되지 않는 Kubernetes 버전을 실행 중입니다.
  - Azure Kubernetes Service 클러스터에 암호화되지 않은 Kubernetes 보안 암호가 있음
- Azure Kubernetes Service 클러스터의 연결성 특성
  - Azure Kubernetes Service 클러스터는 퍼블릭 액세스를 허용합니다.


## Azure Kubernetes Service 클러스터의 잘못된 구성 특성

다음은 Azure Kubernetes Service 클러스터의 잘못된 구성 특성과 제안된 수정 단계입니다.

### Azure Kubernetes Service 클러스터가 지원되지 않는 Kubernetes 버전을 실행 중입니다.

AKS 클러스터가 Microsoft에서 더 이상 지원하지 않는 Kubernetes 버전을 실행 중입니다. 지원되지 않는 Kubernetes 버전은 보안 패치 및 버그 수정 수신을 중지합니다. 그러면 컨트롤 플레인 및 노드 구성 요소에 알려진 취약성이 해결되지 않고 클러스터가 공격에 노출됩니다. 보안 모범 사례에 따라 클러스터를 지원되는 Kubernetes 버전에 유지합니다.

문제 해결: 지원되는 Kubernetes 버전으로 업그레이드

클러스터 컨트롤 플레인 및 노드 풀을 지원되는 Kubernetes 버전으로 업그레이드합니다. 마이너 버전은 건너뛸 수 없으므로 각 마이너 버전을 순차적으로 업그레이드하고 최신 패치를 적용합니다. 업그레이드하기 전에 각 버전의 주요 변경 사항을 검토합니다.

자동 업그레이드를 활성화하여 최신 상태를 유지하는 것이 좋습니다. 자세한 내용은 Microsoft Azure 설명서의 AKS에서 지원되는 Kubernetes 버전을 참조하세요.

### Azure Kubernetes Service 클러스터에 암호화되지 않은 Kubernetes 보안 암호가 있음

기본적으로 클러스터는 고객 제어 키에 의한 암호화 없이 Kubernetes 보안 암호를 etcd 데이터 스토어에 저장합니다. 키 관리 서비스를 사용하여 저장 시 암호화를 사용하지 않으면 기본 etcd 데이터에 액세스할 수 있는 모든 사용자가 자격 증명 및 토큰과 같은 민감한 보안 암호 값을 읽을 수 있습니다. 데이

터 보호 모범 사례에 따라 KMS etcd 암호화를 활성화하여 Kubernetes 보안 암호가 Azure Key Vault의 키로 저장 시 암호화되도록 합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

KMS etcd 암호화 활성화

Azure Key Vault에 저장된 키와 함께 Key Management Service(KMS) etcd 암호화를 사용하도록 클러스터를 구성합니다. 클러스터 자격 증명에 키에 대한 암호화 및 복호화 권한을 부여합니다. 기능을 활성화한 후 기존 보안 암호를 다시 암호화합니다. 키가 손실되지 않도록 키 볼트에서 소프트 삭제 및 제거 보호를 활성화합니다. 자세한 내용은 Microsoft Azure 설명서의 AKS의 KMS etcd 암호화를 참조하세요.

키가 손실되지 않도록 키 볼트에서 소프트 삭제 및 제거 보호를 활성화합니다. 자세한 내용은 Microsoft Azure 설명서의 AKS의 KMS etcd 암호화를 참조하세요.

Azure Key Vault에 보안 암호 저장

민감한 값을 Kubernetes 보안 암호로 저장하지 않으려면 런타임 시 Secrets Store CSI 드라이버의 Azure Key Vault 공급자를 사용하여 Azure Key Vault의 보안 암호, 키 및 인증서를 포드에 탑재합니다. 자세한 내용은 Microsoft Azure 설명서의 Secrets Store CSI 드라이버용 Azure Key Vault 공급자를 참조하세요.

Azure Kubernetes Service 클러스터의 연결성 특성

다음은 Azure Kubernetes Service 클러스터의 연결성 특성과 제안된 수정 단계입니다.

Azure Kubernetes Service 클러스터는 퍼블릭 액세스를 허용합니다.

API 서버는 클러스터의 Kubernetes 컨트롤 플레인과 통신하는 데 사용하는 엔드포인트입니다. API 서버 엔드포인트가 퍼블릭이거나 워크로드가 퍼블릭 로드 밸런서 또는 수신을 통해 노출되는 경우 인터넷에서 클러스터에 연결할 수 있습니다. 퍼블릭 엔드포인트는 공격 표면을 늘리고 Kubernetes API 서버에 대한 무단 액세스 위험을 높입니다. 공격자는 잠재적으로 클러스터 리소스에 액세스하거나 수정하고 민감한 데이터를 읽을 수 있습니다. 보안 모범 사례에 따라 클러스터의 API 서버 및 워크로드에 대한 액세스를 필요한 IP 범위로만 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

API 서버에 대한 액세스 제한

프라이빗 클러스터를 사용하여 가상 네트워크 내에서만 API 서버에 연결할 수 있도록 하거나 퍼블릭 API 서버 엔드포인트에 연결할 수 있는 소스 주소를 제한하도록 승인된 IP 범위를 구성합니다. 자세한 내용은 Microsoft Azure 설명서의 Private Azure Kubernetes Service 클러스터를 참조하세요.

워크로드의 공개 노출 제한

퍼블릭 로드 밸런서 또는 수신을 통해 노출된 서비스를 검토하고 필요하지 않은 퍼블릭 노출을 제한하거나 제거합니다. 인터넷에서 연결해야 하는 워크로드의 경우 제어된 수신 지점에서 내부 로드 밸런서, 네트워크 보안 그룹 규칙 및 웹 애플리케이션 방화벽을 사용합니다. 자세한 내용은 Microsoft Azure 설명서의 AKS에 대한 네트워킹 개념을 참조하세요.

## Azure Graph 사용자의 노출 문제 해결

AWS Security Hub는 Azure Graph 사용자에 대한 노출 조사 결과를 생성할 수 있습니다.

Security Hub 콘솔에서 노출 조사 결과와 관련된 Azure Graph 사용자 및 해당 식별 정보는 조사 결과 세부 정보의 리소스 섹션에 나열됩니다. 프로그래밍 방식으로 Security Hub CSPM API의 GetFindingsV2 작업을 통해 리소스 세부 정보를 검색할 수 있습니다.

노출 조사 결과와 관련된 리소스를 식별한 후 필요하지 않은 경우 리소스를 삭제할 수 있습니다. 필수적이지 않은 리소스를 삭제하면 노출 프로필과 AWS 비용을 줄일 수 있습니다. 리소스가 필수적인 경우 다음 권장 문제 해결 단계를 수행하여 위험을 완화하세요. 문제 해결 주제는 특성 유형에 따라 구분됩니다.

단일 노출 조사 결과에는 여러 문제 해결 주제에서 식별된 문제가 포함됩니다. 반대로, 하나의 문제 해결 주제만 처리하여 노출 조사 결과를 해결하고 심각도 수준을 낮출 수 있습니다. 위험 문제 해결에 대한 접근 방식은 조직의 요구 사항 및 워크로드에 따라 달라집니다.

> **Note**
>
> 이 주제에 제공된 수정 지침에 따라 다른 Microsoft Azure 리소스에서 추가 상담이 필요할 수 있습니다.

목차


- Azure Graph 사용자의 잘못된 구성 특성
  - Azure Graph 사용자와 연결된 역할에 관리 액세스 역할 할당이 있습니다.
  - Azure Graph 사용자에게 MFA가 활성화되어 있지 않습니다.

Azure Graph 사용자의 잘못된 구성 특성

다음은 Azure Graph 사용자의 잘못된 구성 특성과 제안된 수정 단계입니다.

Azure Graph 사용자와 연결된 역할에 관리 액세스 역할 할당이 있습니다.

Azure Graph 사용자에게는 , `Owner` `Contributor`또는와 같은 관리형 Azure 역할 기반 액세스 제어 (Azure RBAC) 역할 할당이 있습니다`User Access Administrator`. 할당은 종종 구독 또는 관리 그룹과 같은 광범위한 범위에 있습니다. 관리 역할 할당은 광범위한 권한을 부여하므로 공격자는 손상된 사용자 계정을 사용하여 환경 전체에서 내부로 이동하거나, 데이터에 액세스하거나, 리소스를 조작할 수 있습니다. 표준 보안 원칙에 따라 최소 권한을 부여하고 권한 있는 관리자 역할 할당을 제한합니다.

문제 해결

다음 작업 중 하나 이상을 수행하여이 노출을 해결합니다.

관리 역할 할당 검토 및 식별

Azure 포털에서 사용자의 역할 할당을 검토합니다. `Owner`에서 와일드카드(*)를 사용하는 사용자 지정 역할에 대해 `User Access Administrator`, `Contributor`또는와 같은 권한이 있는 관리자 역할을 찾습니다`Actions`. 자세한 내용은 Microsoft Azure 설명서의 Azure 역할 할당 나열을 참조하세요.

최소 권한 액세스 구현

불필요한 권한 있는 역할 할당을 제거하고 가장 좁은 범위에서 할당된 최소 권한의 기본 제공 역할로 바꿉니다. 권한이 있는 관리자 역할보다 직무 역할을 선호합니다. 구독 소유자 수를 최소로 유지 - Microsoft는 3개 이하를 권장합니다.

개별 사용자가 아닌 그룹에 역할을 할당합니다. Microsoft Entra Privileged Identity Management를 사용하여 권한이 있는 역할이 스탠딩 액세스 권한을 부여하는 대신 just-in-time의 시간 제한 활성화에 적합하도록 할 수 있습니다. 자세한 내용은 Microsoft Azure 설명서의 Azure RBAC 모범 사례를 참조하세요.

Azure Graph 사용자에게 MFA가 활성화되어 있지 않습니다.

Azure Graph 사용자는 멀티 팩터 인증(MFA) 없이 대화형으로 로그인할 수 있습니다. MFA가 없으면 계정은 암호로만 보호되므로 피싱, 암호 스프레이 및 자격 증명 스터핑 공격에 취약해집니다. 손상된 암호 하나만으로도 공격자가 로그인할 수 있습니다. 표준 보안 원칙에 따라 대화형 로그인을 사용하는 모든 사용자에게 MFA를 요구합니다.

해결 방법: 멀티 팩터 인증 필요

Microsoft Entra 조건부 액세스 정책을 통해 사용자에게 MFA가 필요합니다. 광범위한 적용 범위를 위해 모든 사용자에게 MFA가 필요한 조건부 액세스 정책 또는 보안 기본값을 활성화합니다. 관리자를 위한 전용 정책의 우선 순위를 지정합니다.

가능하면 조건부 액세스 인증 강도를 통해 FIDO2 보안 키, 패스키 또는 Windows Hello for Business와 같은 피싱 방지 방법을 요구합니다. SMS 또는 음성과 같은 피싱 가능한 메서드를 허용하지 마세요. 자세한 내용은 Microsoft Azure 설명서의 멀티 팩터 인증 배포 계획을 참조하세요.

# Security Hub의 미사용 액세스 조사 결과 이해

Security Hub는 IAM Access Analyzer를 사용하여 계정에서 미사용 IAM 권한, 역할, 액세스 키 및 암호를 식별합니다. 이러한 결과는 적극적으로 사용되지 않는 IAM 보안 주체 및 권한을 강조 표시하여 최소 권한 액세스의 보안 모범 사례를 구현하는 데 도움이 됩니다. 이 기능은 모든 Security Hub 고객에게 추가 비용 없이 제공됩니다.

## 미사용 액세스 분석 작동 방식

Security Hub를 활성화하면 서비스가 계정에 서비스 연결 IAM Access Analyzer를 자동으로 생성합니다. 이 분석기는 AWS CloudTrail 활동 데이터와 비교하여 모든 IAM 보안 주체(역할 및 사용자)를 평가하여 90일 룩백 기간 내에 사용되지 않은 보안 주체 및 권한을 결정합니다. 룩백 기간은 구성할 수 없습니다.

IAM Access Analyzer는 24시간마다 모든 활성 조사 결과를 재평가합니다. 이전에 사용하지 않은 보안 주체 또는 권한이 활성화되면 해당 결과가 자동으로 해결됩니다.

미사용 액세스 분석기는 IAM이 글로벌 서비스이므로 미국 동부(버지니아 북부)에서 실행됩니다. Security Hub는 Security Hub를 활성화한 모든 리전에 결과를 복제합니다. 분석기를 실행하기 위해 미국 동부(버지니아 북부)에서 Security Hub를 활성화할 필요가 없습니다.

## 미사용 액세스 조사 결과 유형

Security Hub는 네 가지 유형의 미사용 액세스 조사 결과를 생성합니다.

| 찾기 유형 | 설명 | 평가된 리소스 |
| --- | --- | --- |
| UnusedIAMRole | 90일 룩백 기간 내에 수임되지 않은 IAM 역할입니다. | IAM 역할 |

| 찾기 유형 | 설명 | 평가된 리소스 |
| --- | --- | --- |
| UnusedIAM UserAccessKey | 90일 룩백 기간 내에 API 요청에 서명하는 데 사용되지 않은 IAM 사용자 액세스 키입니다. | IAM 사용자 |
| UnusedIAM UserPassword | 90일 룩백 기간 내에 콘솔 로그인에 사용되지 않은 IAM 사용자 암호입니다. | IAM 사용자 |
| UnusedPermission | 역할 또는 사용자에게 부여되었지만 90일 룩백 기간 내에 호출되지 않은 특정 IAM 작업입니다. | IAM 역할 또는 IAM 사용자 |

## 서비스 연결 분석기

Security Hub가 생성하는 IAM Access Analyzer는 서비스 연결 분석기입니다. IAM Access Analyzer 콘솔에서 볼 수 있지만 Security Hub가 활성화된 동안에는 수정하거나 삭제할 수 없습니다.

모든 리전에서 Security Hub를 비활성화하면 서비스 연결 분석기가 자동으로 삭제됩니다. 자동 삭제에 실패하면 IAM Access Analyzer `DeleteServiceLinkedAnalyzer` API 작업을 호출하여 분석기를 삭제할 수 있습니다. 이 작업은 계정에 대해 Security Hub가 완전히 비활성화된 후에만 성공합니다.

서비스 연결 분석기는 IAM Access Analyzer에서 독립적으로 생성했을 수 있는 고객 관리형 분석기와는 별개입니다. 고객 관리형 분석기를 생성하거나 삭제해도 서비스 연결 분석기에는 영향을 주지 않으며 그 반대의 경우도 마찬가지입니다.

## 미사용 액세스 조사 결과 보기

미사용 액세스 조사 결과는 다른 Security Hub 조사 결과와 함께 Security Hub 콘솔에 표시됩니다. 유형별로 조사 결과를 필터링하여 미사용 액세스 조사 결과만 볼 수 있습니다. 미사용 액세스 조사 결과는 모든 Security Hub 조사 결과에서 사용하는 것과 동일한 형식인 OCSF(Open Cybersecurity Schema Framework)에서 서식이 지정됩니다.

UnusedPermission 조사 결과의 경우 과도하게 허용적인 정책에서 일부 미사용 권한을 제거하지만 전부는 제거하지 않으면 Security Hub는 기존 조사 결과를 닫고 여전히 과도하게 허용적인 경우 수정된 정책에 대한 새 조사 결과를 생성합니다.

미사용 액세스 조사 결과는 IAM Access Analyzer 콘솔에서도 액세스할 수 있습니다. IAM Access Analyzer 콘솔에서 미사용 액세스 조사 결과는 읽기 전용이며 미국 동부(버지니아 북부) 리전에서만 볼 수 있습니다.

## 노출 조사 결과의 미사용 액세스

미사용 액세스 정보는 Security Hub 노출 조사 결과에 컨텍스트 특성으로 표시될 수 있습니다. 리소스에 연결된 IAM 역할에 미사용 권한이 있는 경우 노출 결과에는 보조 컨텍스트로 포함됩니다. 이렇게 하면 취약성의 잠재적 폭파 반경을 이해하는 데 도움이 됩니다. 과도하게 권한이 부여된 IAM 역할이 있는 리소스는 최소 권한이 있는 리소스보다 위험이 높습니다.

다음 리소스 유형은 노출 결과에 미사용 액세스 컨텍스트 특성을 표시할 수 있습니다.

- Amazon Elastic Compute Cloud 인스턴스
- AWS Lambda 함수
- Amazon Elastic Container Service 서비스
- Amazon Elastic Kubernetes Service 클러스터
- IAM 사용자(직접)

노출 결과에 대한 자세한 내용은 섹션을 참조하세요Security Hub의 노출 조사 결과.

### 미사용 권한에 대한 정책 권장 사항

UnusedPermission 조사 결과의 경우 Security Hub는 최소 권한 정책 권장 사항을 생성할 수 있습니다. 이러한 권장 사항은 보안 주체가 실제로 사용하는 권한만 유지하는 범위가 축소된 대체 정책을 보여줍니다. 자세한 내용은 미사용 액세스 조사 결과에 대한 정책 권장 사항 생성 단원을 참조하십시오.

### 가격 책정

서비스 연결 IAM Access Analyzer는 추가 비용 없이 모든 Security Hub 고객에게 제공됩니다. 분석기 또는 미사용 액세스 결과에 대해서는 별도로 요금이 부과되지 않습니다.

## 미사용 액세스 조사 결과에 대한 정책 권장 사항 생성

미사용 권한 조사 결과의 경우 Security Hub는 범위가 축소된 대체 정책을 보여주는 최소 권한 정책 권장 사항을 생성할 수 있습니다. 권장 사항은 IAM 보안 주체에 연결된 각 정책을 평가하고 보안 주체가 실제로 사용한 권한만 유지하는 대체 정책을 생성합니다. 이 기능은 모든 Security Hub 고객에게 추가 비용 없이 제공됩니다.

### 정책 권장 사항의 작동 방식

정책 권장 사항 생성은 비동기 작업입니다. 권장 사항을 생성하고 검색하려면:

1. GetFindingsV2 API 작업을 사용하여 Security Hub에서 미사용 권한 조사 결과를 검색합니다. 조사 결과의 metadata.uid 필드를 기록해 둡니다.
2. 결과의 GenerateRecommendedPolicyV2로를 호출합니다metadata.uid. 이렇게 하면 일반적으로 20초 이내에 완료되는 권장 사항 생성이 시작됩니다.
3. status 필드가를 반환할 metadata.uid 때까지 동일한를 GetRecommendedPolicyV2 사용하여 폴링합니다SUCCEEDED.
4. 응답에는 하나 이상의 권장 단계가 포함됩니다. 각 단계는 CREATE_POLICY (범위 축소 대체 정책 생성 및 연결) 또는 DETACH_POLICY (과잉 권한이 있는 원래 정책 제거) recommendedAction 중 하나의를 지정합니다. CREATE_POLICY 단계의 경우 응답에는 existingPolicy JSON과 recommendedPolicy JSON이 모두 포함되어 있으므로 비교할 수 있습니다.

해당 결과에 대한 권장 사항이 이전에 생성되지 않은 GetRecommendedPolicyV2 경우를 호출하기 GenerateRecommendedPolicyV2 전에를 호출해야 합니다.

## 추천을 생성할 수 있는 사용자

계정 소유자와 위임된 관리자 모두 이러한 API 작업을 호출할 수 있습니다.

- 계정 소유자는 자신의 계정에서 미사용 권한 조사 결과에 대한 권장 사항을 생성하고 볼 수 있습니다.
- 위임된 관리자는 조직 내에서 멤버 계정의 미사용 권한 조사 결과에 대한 권장 사항을 생성하고 볼 수 있습니다.

위임된 관리자가 아니고 조사 결과가 다른 계정에 속하는 경우 API 작업은 AccessDeniedException 오류를 반환합니다.

## 권장 사항 수명 주기

- 권장 사항은 90일 동안 캐시되며 결과가 활성 상태(종료되지 않음)인 한 계속 사용할 수 있습니다. 그러나를 GenerateRecommendedPolicyV2 여러 번 호출하면 캐시가 무효화되고 캐시된 정책을 대체하는 새 작업이 시작됩니다. 조사 결과당 한 GenerateRecommendedPolicyV2 번만 호출합니다.
- 권장 사항은 detach-and-attach 패턴을 따릅니다. 기존 IAM 정책은 수정하지 않습니다. 권장 정책을 검토하고 IAM 콘솔 또는 IAM API를 통해 수동으로 적용합니다.
- 조사 결과가 해결되면(예: 이전에 사용하지 않은 권한이 사용 중이기 때문에) 권장 사항을 더 이상 사용할 수 없습니다.

## 오류 사례

API 작업은 다음과 같은 상황에서 오류를 반환합니다.

- 결과가 해결되었습니다 — `InvalidInputException` (HTTP 400).
- 결과는 미사용 권한 조사 결과(`InvalidInputException`HTTP 400)가 아닙니다.
- IAM 보안 주체는 IAM Identity Center 권한 세트를 통해 생성되었습니다. 권한 세트 보안 주체에 대한 정책은 직접 수정할 수 없습니다. 권장 사항은 설명과 함께 `FAILED` 상태를 반환합니다.
- 호출자는 위임된 관리자가 아니며 결과는 다른 계정`AccessDeniedException`(HTTP 403)에 속합니다.
- 아직 권장 사항이 생성되지 않았으며 먼저 `GenerateRecommendedPolicyV2` `ResourceNotFoundException` (HTTP 404)를 호출`GetRecommendedPolicyV2`하지 않고를 호출합니다.

## 콘솔 사용

Security Hub 콘솔에서 미사용 권한 조사 결과를 보고 수정 탭을 선택하여 정책 권장 사항을 생성할 수 있습니다. 권장 사항이 생성되는 동안 콘솔에 로딩 스피너가 표시됩니다. 권장 사항이 준비되면 미리 보기를 선택하여 현재 정책과 권장 최소 권한 교체를 side-by-side 비교할 수 있습니다. 권장 정책을 JSON 형식으로 복사할 수 있습니다.

## API 참조

- GenerateRecommendedPolicyV2 - 미사용 권한 결과에 대한 최소 권한 정책 권장 사항의 비동기 생성을 시작합니다. 조사 결과의를 입력`metadata.uid`으로 사용합니다. 성공 시 본문이 비어 있는 HTTP 200을 반환합니다.
- GetRecommendedPolicyV2 - 생성된 정책 권장 사항을 검색합니다. 조사 결과의를 입력`metadata.uid`으로 사용합니다. `maxResults` (1~100) 및 `nextToken` 파라미터를 사용한 페이지 매김을 지원합니다. 권장 사항 상태(`IN_PROGRESS`, `SUCCEEDED`또는 `FAILED`), 권장 사항 단계, 리소스 ARN 및 오류를 반환합니다.

자세한 API 설명서는 Security Hub API 참조를 참조하세요.

# Security Hub의 네트워크 스캔

네트워크 스캔은 클라우드 리소스에서 활성 네트워크 연결성 테스트를 수행하는 Security Hub의 옵트인 기능입니다. 컨트롤 플레인 분석은 보안 그룹, 네트워크 액세스 제어 목록(NACLs) 및 라우팅 테이블을 평가하여 연결할 수 있는 항목을 결정합니다. 네트워크 스캔은 실제로 도달할 수 있는 것을 감지하여 더욱 발전합니다. 계정 외부의 리소스를 프로브하여 열린 포트와 실행 중인 서비스를 식별합니다.

모든 스캔은 AWS소유 IP 주소에서 시작되며 인터넷에서이 리소스에 연결할 수 있습니까?라는 두 가지 질문에 답합니다. 연결 가능한 경우 실행 중인 항목은 무엇입니까? 네트워크 스캔은 결과를 스캔 증거와 함께 Security Hub에 독립 실행형 OCSF 조사 결과로 게시합니다.

## 지원되는 리소스 유형

네트워크 스캔은 다음 리소스 유형을 지원합니다.

| 클라우드 공급자 | 리소스 유형 |
|---|---|
| AWS | EC2 인스턴스(퍼블릭 IP 사용) |
| AWS | 탄력적 IP(EIP) |
| AWS | Network Load Balancer(NLB) |
| AWS | Application Load Balancer(ALB) |
| AWS | Classic Load Balancer(CLB) |
| Azure | 퍼블릭 IP 주소 |

> **Note**
>
> 네트워크 스캔은 각 리소스 유형을 독립적으로 스캔합니다. 로드 밸런서의 경우 Network Scanning은 DNS 이름을 확인하고 스캔합니다. 네트워크 스캔은 자체 퍼블릭 IP 또는 EIP가 있는 경우에만 로드 밸런서 뒤의 개별 EC2 인스턴스를 스캔합니다.

# 네트워크 스캔 활성화

네트워크 스캔을 활성화하려면 계정에서 Security Hub를 활성화해야 합니다. 구성 정책을 통해 또는 개별 계정에 대해 네트워크 스캔을 활성화할 수 있습니다.

조직 계정(권장) - 구성 정책을 생성하거나 편집하여 조직의 계정 및 리전에서 네트워크 스캔을 활성화합니다. 구성 정책 편집에 대한 자세한 내용은 구성 정책 편집을 참조하세요. 구성 정책을 통해 네트워크 스캔을 활성화하면 멤버 계정이 기능을 끌 수 없습니다.

개별 계정 - 구성 정책에서 관리하지 않는 계정의 경우 다음 방법 중 하나를 사용하여 네트워크 스캔을 활성화할 수 있습니다.

> **Note**
>
> 네트워크 스캔을 활성화하면 Security Hub가 AWS 환경 및 Azure 환경의 리소스에 대해 활성 네트워크 스캔을 수행할 수 있는 권한을 부여합니다. 여기에는 TCP 포트 연결 시도, 애플리케이션 및 프로토콜 식별, 서비스 배너, HTTP 헤더 및 TLS 인증서 메타데이터 모음이 포함됩니다.

### Security Hub console

네트워크 스캔을 활성화하려면

1. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 일반 설정을 선택합니다.
3. 네트워크 스캔 섹션을 찾습니다.
4. 활성화를 선택합니다.
5. 활성 네트워크 스캔을 계속하려면 권한 부여를 확인합니다.

### Security Hub API

기능 이름 로 `EnableSecurityHubFeatureV2` API를 호출합니다`NETWORK_SCANNING`.

> **Note**
>
> 네트워크 스캔이 이미 활성화된 경우이 API를 호출하면 200 응답이 반환됩니다. 서비스는 원래 활성화에서 `UpdatedAt` 타임스탬프를 유지합니다.

AWS CLI

다음 명령을 실행하여 네트워크 스캔을 활성화합니다.

```
aws securityhub enable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

## 네트워크 스캔 작동 방식

네트워크 스캔을 활성화하면 다음이 발생합니다.

- 네트워크 스캔은 기능을 활성화한 후 약 24시간 이내에 기존 리소스를 스캔합니다.
- Network Scanning은 Security Hub가 생성된 리소스에 대한 알림을 받은 직후 새 리소스를 스캔합니다.
- 네트워크 스캔은 특정 적격 컨트롤 플레인 변경이 스캔 적격 리소스에 적용되면 리소스를 다시 스캔합니다.
- 네트워크 스캔은 약 12시간마다 활성 리소스를 다시 스캔하여 연결성 변경을 감지합니다.

임시 또는 단기 리소스는 종료되기 전에 스캔되지 않을 수 있습니다.

## 네트워크 스캔 조사 결과

네트워크 스캔은 OCSF 확장을 사용하여 AWS OCSF(Open Cybersecurity Schema Framework) 형식으로 조사 결과를 게시하고 다른 Security Hub 조사 결과와 함께 표시됩니다. 네트워크 스캔은 리소스에 연결할 수 있는 포트가 있는지 여부에 관계없이 조사 결과를 생성합니다. 지원되는 리소스 유형에 대한 결과가 없는 경우 네트워크 스캔이 아직 리소스를 스캔하지 않은 것입니다.

### 연결 가능한 포트에 대한 결과

각 결과는 특정 리소스 및 주소 조합에서 연결할 수 있는 단일 포트를 나타냅니다. OCSF 결과의 `port_scan_result_list` 섹션에는 스캔 결과가 포함되어 있습니다. 다음 예제에서는 연결 가능한 리소스에 대해 반환된 정보를 보여줍니다.

```
"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
    }
  ],
```

## 열린 포트 없음에 대한 정보 조사 결과

네트워크 스캔은 리소스에서 열린 포트를 감지하지 못하면 결과를 생성합니다. 이 결과의 심각도는 `Informational` 이며 조치가 필요하지 않습니다. 네트워크 스캔이 리소스를 스캔했는지 확인합니다.

리소스를 삭제하거나 Network Scanning이 리소스에서 열린 포트를 감지할 때까지 Security Hub에서 정보 조사 결과가 열린 상태로 유지됩니다. 네트워크 스캔이 정보 조사 결과를 사용하여 리소스의 열린 포트를 식별하면 정보 조사 결과를 닫습니다. 그런 다음 열린 각 포트에 대한 결과를 생성합니다.

열려 있지 않은 포트에 대한 정보 조사 결과는 네트워크 스캔이 현재 지원하는 포트를 포함합니다. 지원되는 포트 목록은 섹션을 참조하세요the section called “지원되는 포트”.

## 수명 주기 이벤트 찾기

다음 표에서는 네트워크 스캔 결과의 수명 주기를 설명합니다.

| Event | 발생한 상황 |
| --- | --- |
| 열린 포트가 감지되지 않음 | 네트워크 스캔은 조치가 필요하지 않은 `Informational` 결과를 생성합니다. |
| 정보 조사 결과를 사용하여 리소스에서 열린 포트가 감지됨 | 네트워크 스캔은 정보 조사 결과를 닫고 열린 각 포트에 대한 조사 결과를 생성합니다. |
| 포트가 먼저 연결 가능한 것으로 감지됨 | 네트워크 스캔은 새 결과를 생성하고 게시합니다. |
| 재스캔 시 포트에 계속 연결할 수 있음(변경 없음) | 네트워크 스캔은 조사 결과를 주기적으로 새로 고칩니다. |
| 포트는 여전히 연결할 수 있지만 증거가 변경되었습니다. | Network Scanning은 업데이트된 증거와 함께 조사 결과를 다시 게시합니다. |
| 포트에 더 이상 연결할 수 없음 | 다음 재스캔에서 포트에 연결할 수 없음이 확인될 때까지 결과는 열린 상태로 유지됩니다. |
| 리소스 종료 또는 삭제됨 | 네트워크 스캔은 `activity_name` 속성을 로 설정하여 리소스에 대한 모든 조사 결과를 닫습니다. `Close` |
| 리소스에서 제거된 IP 주소 | 네트워크 스캔은 해당 특정 IP에 대한 조사 결과를 닫습니다. |
| 네트워크 스캔 비활성화됨 | 네트워크 스캔은 새로운 결과를 생성하지 않습니다. 기존 결과는 만료될 때까지 유지됩니다. |
| Security Hub 비활성화됨 | 더 이상 결과에 액세스할 수 없습니다. |

포트에 간헐적으로 연결할 수 있는 경우 네트워크 스캔은 스캔 시 긍정적인 증거를 기반으로 조사 결과를 생성합니다. 문제를 해결한 후(예: 방화벽 규칙을 닫거나 서비스를 중지하여) 네트워크 스캔은 다음 스캔에서 조사 결과를 닫습니다.

네트워크 스캔을 비활성화해도 결과가 즉시 닫히지는 않습니다. 기존 조사 결과는 일반적인 Security Hub 조사 결과 수명 주기가 끝날 때까지 계속 표시됩니다.

> **Note**
>
> 탄력적 IP 주소(EIP)를 Amazon EC2 인스턴스에 연결하면 네트워크 스캔이 EIP 리소스에 대한 조사 결과를 생성합니다. EIP는 주소를 소유한 최상위 IP 리소스입니다. Network Load Balancer(NLB) 리소스의 경우 DNS 이름과 연결된 EIPs는 고유한 네트워크 진입점이므로 Network Scanning은 각각에 대해 별도의 결과를 생성합니다.

## 스캔 증거

네트워크 스캔에서 포트에 연결할 수 있는 것으로 감지되면 결과에는 연결 가능한 서비스에 대한 증거가 포함됩니다. 다음과 같은 유형의 증거를 수집할 수 있습니다.

TCP 배너

SSH 버전 문자열과 같이 연결 시 서비스가 전송하는 초기 바이트입니다.

HTTP 메타데이터

응답 헤더 및 HTTP 상태 코드.

TLS 인증서

일반 이름(CN), 발급자, 만료 날짜 및 자체 서명 상태입니다.

서비스 감지

포트에서 실행되는 식별된 애플리케이션 또는 프로토콜입니다.

## 스캔에서 리소스 제외

네트워크 스캔에서 리소스를 제외하려면 `SecurityHubNetworkScanExclusion` 리소스에 태그 키를 추가합니다. 태그 값은 임의의 값이거나 비어 있을 수 있습니다.

스캔 가능한 퍼블릭 IP를 사용하여 실제 리소스에 태그를 적용해야 합니다.

- EC2 인스턴스에 연결된 EIP의 경우 - EC2 인스턴스가 아닌 EIP에 태그를 지정합니다.
- 퍼블릭 IP(EIP 없음)만 있는 EC2 인스턴스의 경우 - EC2 인스턴스에 태그를 지정합니다.
- 로드 밸런서의 경우 - 로드 밸런서와 대상에 개별 퍼블릭 IPs 태그를 지정합니다.

제외 태그를 추가하면 네트워크 스캔이 향후 스캔을 중지하고 해당 리소스에 대한 활성 조사 결과를 닫습니다. 태그를 제거하면 리소스가 다시 스캔할 수 있습니다.

## 지원되는 포트

네트워크 스캔은 적격 리소스에서 다음과 같은 잘 알려진 TCP 포트를 스캔합니다.

```
21, 22, 23, 25, 53, 80, 110, 143, 443, 445, 1433, 3306, 3389, 5432,
5900, 6379, 8080, 8443, 9200, 27017
```

## 다중 클라우드 지원

네트워크 스캔은 Azure 퍼블릭 IP 주소를 지원합니다. Azure 리소스를 스캔하려면 Azure 환경에 대한 Security Hub 커넥터를 생성합니다. Microsoft Azure와 통합에 대한 자세한 내용은 Security Hub와 Microsoft Azure 통합을 참조하세요.

Azure 리소스에 대한 스캔 동작, 증거 및 결과는 AWS 리소스와 동일합니다. 조사 결과는 적절한 클라우드 공급자 및 리전 메타데이터가 있는 AWS 조사 결과와 함께 표시됩니다.

## 리전 가용성

네트워크 스캔은 Security Hub를 사용할 수 있는 상용 AWS 리전에서 사용할 수 있습니다.

## 네트워크 스캔 비활성화

조직에서 구성 정책을 사용하는 경우 위임된 관리자는 구성 정책을 편집하여 특정 계정 및 리전에서 네트워크 스캔을 비활성화할 수 있습니다. 구성 정책 편집에 대한 자세한 내용은 구성 정책 편집을 참조하세요. 정책을 편집할 때 네트워크 스캔 기능을 선택하고 비활성화를 선택한 다음 스캔을 끄려는 계정 및 리전을 지정합니다.

구성 정책에서 관리하지 않는 계정의 경우 다음 방법 중 하나를 사용하여 네트워크 스캔을 비활성화할 수 있습니다.

Security Hub console

네트워크 스캔을 비활성화하려면

1. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 일반 설정을 선택합니다.
3. 네트워크 스캔 섹션을 찾습니다.
4. 비활성화를 선택합니다.
5. 네트워크 스캔을 비활성화할지 확인합니다.

Security Hub API

기능 이름 로 `DisableSecurityHubFeatureV2` API를 호출합니다`NETWORK_SCANNING`.

AWS CLI

다음 명령을 실행하여 네트워크 스캔을 비활성화합니다.

```
aws securityhub disable-security-hub-feature-v2 --feature-name NETWORK_SCANNING
```

네트워크 스캔을 비활성화하는 경우:

- 네트워크 스캔은 새 스캔을 트리거하지 않습니다.
- 기존 조사 결과는 일반적인 Security Hub 조사 결과 수명 주기가 끝날 때까지 계속 표시됩니다.
- 네트워크 스캔은 이미 진행 중인 모든 스캔을 완료합니다.

# Security Hub의 자동화

Security Hub에는 사양에 따라 조사 결과를 자동으로 수정하고 조치를 취하는 기능이 있습니다.

Security Hub는 현재 다음과 같은 유형의 자동화를 지원합니다.

- 자동화 규칙 – 정의한 기준에 따라 거의 실시간으로 조사 결과를 자동으로 업데이트하고, 숨기고, 티켓팅 도구로 전송합니다.
- 자동 응답 및 해결 – 특정 조사 결과 및 인사이트에 대해 취해야 할 자동 조치를 정의하는 사용자 지정 Amazon EventBridge 규칙을 생성합니다.

자동화 규칙은 개방형 사이버 보안 스키마 프레임워크(OCSF)의 결과 필드를 자동으로 업데이트하려는 경우에 유용합니다. 예를 들어 자동화 규칙을 사용하여 특정 태그가 지정된 리소스에 대한 조사 결과의 심각도 수준을 업데이트할 수 있습니다. 자동화 규칙을 사용하면 특정 태그와 관련된 각 조사 결과의 심각도 수준을 수동으로 업데이트할 필요가 없습니다. 조사 결과가 특정 속성과 일치할 경우 Jira Cloud 및 ServiceNow와 같은 도구에서 티켓을 생성하도록 자동화 규칙을 구성할 수 있습니다. 티켓은 Security Hub에 도착하는 즉시 결과에서 생성됩니다.

EventBridge 규칙은 특정 결과에 대해 Security Hub 외부에서 조치를 취하거나 문제 해결 또는 추가 조사를 위해 타사 도구로 특정 결과를 보내려는 경우에 유용합니다. 이 규칙은 AWS Lambda 함수 호출 또는 특정 결과에 대한 Amazon Simple Notification Service(Amazon SNS) 주제 알림과 같은 지원되는 작업을 트리거하는 데 사용할 수 있습니다.

자동화 규칙은 EventBridge 규칙보다 먼저 적용됩니다. 즉, EventBridge로 전송되기 전에 자동화 규칙이 트리거되고 조사 결과가 업데이트됩니다. 그러면 EventBridge 규칙이 업데이트된 조사 결과에 적용됩니다.

## Security Hub의 자동화 규칙

Security Hub를 사용하면 조사 결과 세부 정보 업데이트, 서드 파티 통합에 대한 티켓 생성과 같은 작업을 자동화할 수 있습니다.

### 자동화 규칙 및 AWS 리전

자동화 규칙은 하나의에서 생성한 AWS 리전 다음 구성된 모든에 적용할 수 있습니다 AWS 리전. 리전 집계를 사용하는 경우 홈 리전에서만 규칙을 생성할 수 있습니다. 홈 리전에서 규칙을 생성할 때 규칙 기준에서 특정 연결된 리전을 제외하지 않는 한 정의한 모든 규칙이 모든 연결된 리전에 적용됩니다. 연결된 리전이 아닌 모든 리전에 대해 자동화 규칙을 생성해야 합니다.

### 규칙 작업 및 기준

Security Hub의 자동화 규칙은 기준을 사용하여 Security Hub 조사 결과의 OCSF 속성을 참조합니다. 예를 들어 CreateAutomationRuleV2의 `Criteria` 파라미터에 지원되는 필터는 GetFindingsV2의 `Filters` 파라미터에 지원되는 필터와 일치합니다. 즉, 자동화 규칙에 사용되는 필터를 사용하여 조사 결과를 가져올 수 있습니다. Security Hub는 자동화 규칙 기준에 대해 다음 OCSF 필드를 지원합니다.

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
| --- | --- | --- | --- |
| `activity_id` | `Activity ID` | `Eq (equal-to), Gte (greater-` | `Number` |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
| --- | --- | --- | --- |
| | | than-equal), Lte (less-than-equal) | |
| activity_name | Provider status | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| class_name | Finding class name | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| cloud.account.name | Finding account name | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| cloud.account.uid | Account ID | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| cloud.provider | Cloud provider | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| cloud.region | Region | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| 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 |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| compliance.standards | Applicable standards | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| 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 |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| finding_info.first_seen_time_dt | First observed at | Start, End, DateRange | Date (formatted as 2022-12-01T21:47:39.269Z) |
| 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 |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| finding_info.related_events.uid | Related findings ID | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| 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 |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| finding_info.uid | Provider finding ID | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| 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 |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| remediation.references | Recommendation URL | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| 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 |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| resources .owner.org.uid | Organization | EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS | String |
| resources .provider | Cloud provider | EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS | String |
| resources .region | Resource region | EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS | String |
| resources.tags | Resource tags | EQUALS | Map |
| resources.type | Resource type | EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS | String |
| resources.uid | Resource ID | EQUALS, PREFIX, CONTAINS, NOT_EQUAL S, PREFIX_NO T_EQUALS | String |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| vendor_attributes.severity | Provider severity | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| 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 |

| OCSF 필드 | 콘솔 필터 값 | 필터 연산자 | 필드 유형 |
|---|---|---|---|
| vulnerabilities.cve.uid | Vulnerability ID | EQUALS, PREFIX, CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | String |
| 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 |

문자열 필드로 레이블이 지정된 기준의 경우, 동일한 필드에 다른 필터 연산자를 사용하면 평가 로직에 영향을 미칩니다. 자세한 내용은 Security Hub API 참조의 StringFilter를 참조하세요.

각 기준은 일치하는 결과를 필터링하는 데 사용할 수 있는 최대 값 수를 지원합니다. 각 기준의 제한은 Security Hub API 참조의 OcsfFindingFilters를 참조하세요

업데이트할 수 있는 OCSF 필드

다음은 자동화 규칙을 사용하여 업데이트할 수 있는 OCSF 필드입니다.

- Comment
- SeverityId
- StatusId

## 자동화 규칙이 조사 결과를 평가하는 방법

자동화 규칙은 규칙을 생성한 후 Security Hub가 생성하거나 수집하는 신규 및 업데이트된 조사 결과를 평가합니다.

자동화 규칙은 공급자가 제공한 원본 조사 결과를 평가합니다. 공급자는 Security Hub와의 통합을 통해 새로운 조사 결과를 제공하고 기존 조사 결과를 업데이트할 수 있습니다. BatchUpdateFindingsV2 작업을 통해 규칙을 생성한 후 결과 필드를 업데이트하면 규칙이 트리거되지 않습니다. 자동화 규칙을 생성하고 동일한 결과 필드에 영향을 미치는 BatchUpdateFindingsV2 업데이트를 수행하는 경우, 마지막 업데이트는 해당 필드의 값을 설정합니다. 다음의 예제를 참조하세요.

BatchUpdateFindingsV2을(를) 사용하여 조사 결과의 Status 필드를 New에서 In Process(으)로 업데이트합니다. GetFindingsV2을(를) 직접 호출하는 경우, 이제 Status 필드의 값은 In Process입니다. 결과의 Status 필드를 New에서 Suppressed(으)로 변경하는 자동화 규칙을 생성합니다(규칙이 BatchUpdateFindingsV2(으)로 수행된 업데이트는 무시한다는 점을 기억하세요). 조사 결과 공급자는 조사 결과를 업데이트하고 Status 필드를 New로 변경합니다. GetFindingsV2를 직접 호출하는 경우, 자동화 규칙이 적용되었고 규칙이 조사 결과에 대해 마지막으로 수행된 작업이므로 이제 Status 필드의 값은 Suppressed입니다.

Security Hub 콘솔에서 규칙을 생성하거나 편집하면 콘솔에 규칙 기준과 일치하는 조사 결과의 미리 보기가 표시됩니다. 자동화 규칙은 결과 공급자가 보낸 원래 결과를 평가하는 반면 콘솔 미리 보기는 GetFindingsV2 API 작업에 대한 응답에 표시되는 최종 상태의 결과를 반영합니다(즉, 규칙 작업 또는 기타 업데이트가 결과에 적용된 후).

## 자동화 규칙 순서 지정 방법

각 자동화 규칙에는 규칙 순서가 할당됩니다. 이는 Security Hub에서 자동화 규칙을 적용하는 순서를 결정하며, 여러 규칙이 동일한 결과 또는 결과 필드와 관련된 경우, 중요해집니다.

여러 규칙 작업이 동일한 결과 또는 결과 필드와 관련된 경우, 규칙 순서의 숫자 값이 가장 높은 규칙이 마지막에 적용되어 궁극적인 효과를 발휘합니다.

Security Hub 콘솔에서 규칙을 생성하면 Security Hub는 규칙 생성 순서에 따라 규칙 순서를 자동으로 할당합니다. 첫 번째로 생성하는 규칙의 규칙 순서는 1입니다. 2개 이상의 규칙이 존재하는 경우 이후에 생성되는 각 규칙은 규칙 순서에 사용할 수 있는 다음으로 가장 높은 숫자 값을 갖게 됩니다.

CreateAutomationRuleV2 API 또는를 통해 규칙을 생성하면 AWS CLI Security Hub는 `RuleOrder` 먼저에 대해 숫자 값이 가장 낮은 규칙을 적용합니다. 그런 다음 다음 규칙을 오름차순으로 적용합니다. 여러 조사 결과에 동일한 `RuleOrder`가 있는 경우, Security Hub는 `UpdatedAt` 필드에 이전 값이 있는 규칙을 먼저 적용합니다(즉, 가장 최근에 편집된 규칙이 마지막에 적용됨).

언제든지 규칙 순서를 변경할 수 있습니다.

규칙 순서의 예제:

규칙 A(규칙 순서는 **1**):

- 규칙 A 기준
  - `ProductName` = `Security Hub CSPM`
  - `Resources.Type`은(는) `S3 Bucket`
  - `Compliance.Status` = `FAILED`
  - `RecordState`은(는) `NEW`
  - `Workflow.Status` = `ACTIVE`
- 규칙 A 작업
  - `Confidence`을(를) `95`(으)로 업데이트
  - `Severity`을(를) `CRITICAL`(으)로 업데이트
  - `Comment`을(를) `This needs attention`(으)로 업데이트

규칙 B(규칙 순서는 **2**):

- 규칙 B 기준
  - `AwsAccountId` = `123456789012`
- 규칙 B 작업
  - `Severity`을(를) `INFORMATIONAL`(으)로 업데이트

먼저, 규칙 A 작업이 규칙 A 기준과 일치하는 Security Hub 조사 결과에 적용됩니다. 다음으로, 규칙 B 작업이 지정된 계정 ID를 가진 Security Hub 조사 결과에 적용됩니다. 이 예제에서는 규칙 B가 마지막

에 적용되므로 지정된 계정 ID의 조사 결과에서 `Severity`의 최종 값은 `INFORMATIONAL`입니다. 규칙 A 작업에 따라 일치하는 조사 결과에서 `Confidence`의 최종 값은 `95`입니다.

### 타사 통합

자동화 규칙을 사용하여 Jira Cloud 및 ServiceNow ITSM의 통합에 대한 티켓을 생성할 수 있습니다. 자세한 내용은 서드 파티 통합을 위한 규칙 생성을 참조하세요.

## 자동화 규칙이 작동하지 않는 시나리오

다음은 자동화 규칙이 작동하지 않는 시나리오입니다.

- 독립형 계정이 위임된 관리자가 있는 조직의 멤버가 되는 경우
- 조직 관리 계정이 위임된 관리자를 제거하고 새 위임된 관리자를 설정하는 경우
- 연결되지 않은 리전이 연결된 리전이 되면 위임된 관리자 또는 독립 실행형 계정에 대한 집계자 구성이 변경됩니다.

이러한 시나리오 중에 조직의 구성원은 AWS CLI 또는 APIs.

연결 해제된 리전이 연결된 리전이 되면 위임된 관리자 또는 독립 실행형 계정은 목록, 가져오기 및 삭제 작업을 사용하여 연결된 리전의 리소스를 관리할 수 있습니다.

## Security Hub에서 자동화 규칙 생성

이 주제에서는 자동화 규칙을 생성하는 방법을 설명합니다. 자동화 규칙을 사용하여 조사 결과 세부 정보를 업데이트하거나 서드 파티 통합에 대한 티켓을 생성할 수 있습니다. 자동화 규칙을 적용하려는 AWS 리전 에서 개별적으로 생성해야 합니다. 그러나 집계 리전에서 자동화 규칙을 생성하면 모든 리전에 적용됩니다. 그렇지 않으면 연결되지 않은 리전에서 자동화 규칙을 생성하면 해당 리전에서만 적용됩니다.

조사 결과 세부 정보를 업데이트하는 규칙 생성

다음 절차에서는 조사 결과 세부 정보를 업데이트하는 규칙을 생성하는 방법을 설명합니다.

1. AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 관리에서 자동화를 선택합니다.
3. 규칙 생성을 선택합니다.

4. 세부 정보에 자동화 규칙의 이름을 입력합니다.

   - (선택 사항) 자동화 규칙에 대한 설명을 입력합니다.

5. 작업에서 조사 결과 세부 정보 업데이트를 선택합니다. 검색 창에서 기준을 검색하고 추가할 수 있습니다. 기준과 일치하는 조사 결과가 있는지 확인하려면 일치하는 조사 결과 미리 보기를 선택합니다.
6. 조사 결과 세부 정보 업데이트에서 조사 결과가 기준과 일치할 때 업데이트할 조사 결과 세부 정보를 하나 이상 선택합니다. 심각도, 상태 또는 설명을 선택할 수 있습니다.
7. 규칙 설정에서 활성화됨 또는 비활성화됨을 선택합니다. 활성화됨을 선택하면 자동화 규칙이 활성화되고 새 조사 결과가 처리됩니다. 비활성화됨을 선택하면 자동화 규칙이 비활성화되고 결과가 처리되지 않습니다.
8. (선택 사항) 태그에서 새 태그 추가를 선택하고 자동화 규칙에 적용할 키-값 페어를 입력합니다.
9. 규칙 생성을 선택합니다.

### 서드 파티 통합을 위한 규칙 생성

다음 절차에서는 서드 파티 통합에 대한 티켓을 생성하는 규칙을 생성하는 방법을 설명합니다. Security Hub CSPM이 지원하는 통합에 대한 자세한 내용은 Security Hub CSPM의 서드 파티 통합을 참조하세요.

1. AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 관리에서 자동화를 선택합니다.
3. 규칙 생성을 선택합니다.
4. 세부 정보에 자동화 규칙의 이름을 입력합니다.

   - (선택 사항) 자동화 규칙에 대한 설명을 입력합니다.

5. 작업에서 티켓 생성을 선택합니다. 검색 창에서 기준을 검색하고 추가할 수 있습니다. 기준과 일치하는 조사 결과가 있는지 확인하려면 일치하는 조사 결과 미리 보기를 선택합니다.
6. 티켓 생성 아래의 드롭다운에서 IT 티켓팅 통합을 선택한 다음 통합 추가를 선택합니다.
7. 규칙 설정에서 활성화됨 또는 비활성화됨을 선택합니다. 활성화됨을 선택하면 자동화 규칙이 활성화되고 새 조사 결과가 처리됩니다. 비활성화됨을 선택하면 자동화 규칙이 비활성화되고 결과가 처리되지 않습니다.
8. (선택 사항) 태그에서 새 태그 추가를 선택하고 자동화 규칙에 적용할 키-값 페어를 입력합니다.
9. 규칙 생성을 선택합니다.

## Security Hub에서 자동화 규칙 세부 정보 보기

이 주제에서는 자동화 규칙에 대한 세부 정보를 보는 방법을 설명합니다. 자동화 규칙에서 다음 세부 정보를 볼 수 있습니다.

- 이름 및 설명
- 작업 및 기준
- 규칙 상태 및 기존 조사 결과
- Tags

자동화 규칙에 대한 세부 정보를 보려면

1. AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 관리에서 자동화를 선택합니다. 이 화면에는 생성된 자동화 규칙이 모두 표시됩니다.
3. 보려는 자동화 규칙을 선택합니다. 세부 정보 보기를 선택합니다. 또는, 보려는 자동화 규칙의 이름을 선택할 수 있습니다.

## Security Hub에서 규칙 순서 업데이트

이 주제에서는 콘솔에서 자동화 규칙의 규칙 순서를 업데이트하는 방법을 설명합니다. 자동화 규칙의 기준을 편집하려면 Security Hub에서 자동화 규칙 편집을 참조하세요.

모든 자동화 규칙의 규칙 순서를 업데이트하지 않고 하나의 자동화 규칙의 규칙 순서를 업데이트할 수는 없습니다. 예를 들어 규칙 A(1), 규칙 B(2), 규칙 C(3), 규칙 D(4) 등 4가지 자동화 규칙이 있습니다. 규칙 D를 먼저 적용하려고 합니다. 이렇게 하려면 숫자를 4에서 1로 변경합니다. 결과적으로 규칙 A는 2, 규칙 B는 3, 규칙 C는 4가 할당됩니다.

자동화 규칙의 규칙 순서를 업데이트하려면

1. AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 관리에서 자동화를 선택합니다.
3. 편집할 자동화 규칙을 선택합니다. 순서에서 순서 번호 옆의 연필 아이콘을 선택합니다. 화살표를 사용하여 새 순서 번호를 확인합니다. ✓ 아이콘을 선택하여 확인합니다. 취소하려면 X 아이콘을 선택합니다. 또는 순서 변경을 선택하여 자동화 규칙을 아래, 위 또는 목록 맨 위로 이동할 수 있습니다.

## Security Hub에서 자동화 규칙 비활성화

이 주제에서는 자동화 규칙을 비활성화하는 방법을 설명합니다. 자동화 규칙을 비활성화하면 Security Hub는 규칙 적용을 중지합니다. 자동화 규칙을 생성한 AWS 리전 에서 언제든지 자동화 규칙을 비활성화할 수 있습니다.

규칙을 비활성화하려면

1. AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 관리에서 자동화를 선택합니다.
3. 비활성화하려는 자동화 규칙을 선택합니다. 상태 아래에서 활성화됨 옆의 연필 아이콘을 선택합니다. 드롭다운을 선택한 다음 비활성화됨을 선택합니다. ✓ 아이콘을 선택하여 확인합니다. 취소하려면 X 아이콘을 선택합니다. 작업 드롭다운에서 비활성화를 선택할 수도 있습니다.

## Security Hub에서 자동화 규칙 활성화

이 주제에서는 자동화 규칙을 활성화하는 방법을 설명합니다. 자동화 규칙을 활성화하면 Security Hub가 규칙 적용을 재개합니다. 자동화 규칙을 생성한 AWS 리전 에서 언제든지 자동화 규칙을 활성화할 수 있습니다.

규칙을 활성화하려면

1. AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 관리에서 자동화를 선택합니다.
3. 활성화하려는 자동화 규칙을 선택합니다. 상태 아래에서 비활성화됨 옆의 연필 아이콘을 선택합니다. 드롭다운을 선택한 다음 활성화됨을 선택합니다. ✓ 아이콘을 선택하여 확인합니다. 취소하려면 X 아이콘을 선택합니다. 작업 드롭다운에서 활성화를 선택할 수도 있습니다.

## Security Hub에서 자동화 규칙 복제

이 주제에서는 자동화 규칙을 복제하는 방법을 설명합니다. 자동화 규칙을 처음부터 생성하지 않으려는 경우 복제하면 시간을 절약할 수 있습니다. 자동화 규칙을 복제할 때 세부 정보, 작업, 규칙 설정 및 태그를 업데이트할 수 있습니다. 자동화 규칙을 생성한 AWS 리전 에서 자동화 규칙을 편집할 수 있습니다.

규칙을 복제하려면

1. AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 자동화를 선택합니다.
3. 복제하려는 자동화 규칙을 선택합니다. 그런 다음 작업을 선택하고 복제를 선택합니다.
4. 변경 사항을 적용하고 검토한 다음 규칙 생성을 선택합니다.

## Security Hub에서 자동화 규칙 편집

이 주제에서는 자동화 규칙을 편집하는 방법을 설명합니다. 자동화 규칙을 생성한 AWS 리전 에서 자동화 규칙을 편집할 수 있습니다.

자동화 규칙에서 다음 항목을 편집할 수 있습니다.

- 이름 및 설명
- 작업
- 규칙 설정

자동화 규칙의 태그는 편집할 수 없습니다.

규칙을 편집하려면

1. AWS 계정에 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창의 관리에서 자동화를 선택합니다.
3. 편집할 자동화 규칙을 선택합니다. 작업을 선택한 후 편집을 선택합니다.
4. 편집을 수행하고 편집 내용을 검토합니다.
5. 변경 사항 저장을 선택합니다.

## Security Hub에서 자동화 규칙 삭제

이 주제에서는 자동화 규칙을 삭제하는 방법을 설명합니다. 자동화 규칙을 생성한 AWS 리전 에서 자동화 규칙을 삭제할 수 있습니다.

규칙 삭제

1. AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 자동화를 선택합니다.
3. 삭제할 자동화 규칙을 선택합니다. [ Actions]를 선택한 후 [Delete]를 선택합니다.
4. 삭제를 선택합니다.

## EventBridge의 자동화 규칙

Amazon EventBridge의 자동화 규칙을 사용하여 Security Hub 조사 결과에 응답할 수 있습니다. Security Hub는 거의 실시간으로 조사 결과를 EventBridge에 이벤트로 전송합니다. 이벤트가 규칙과 일치할 때 수행할 자동화된 작업을 나타내는 기본 규칙을 작성할 수 있습니다. 자동으로 트리거할 수 있는 작업은 다음과 같습니다.

- EventBridge에서 API 대상 구성.
- Amazon EC2 Run Command 간접 호출
- Lambda 함수 호출
- Step Functions 상태 시스템 간접 호출
- SNS 주제 또는 Amazon SQS 대기열 알림
- Kinesis Data Streams로 이벤트 릴레이
- 타사 티켓팅, 채팅, SIEM 또는 인시던트 대응 및 관리 도구에 조사 결과 전송
- 다른 AWS 계정의 EventBridge 버스로 이벤트 전송

Security Hub는 새로운 조사 결과와 업데이트된 조사 결과를 EventBridge에 이벤트로 전송합니다. 그러면 각 Security Hub 이벤트에 응답하도록 EventBridge 규칙을 구성합니다. 자세한 내용은 EventBridge 사용 설명서의 EventBridge란?을 참조하세요.

> **Note**
>
> Security Hub CSPM의 결과에 대해 EventBridge 규칙이 정의된 경우 규칙이 Security Hub에 대해 정의된 규칙과 겹칠 수 있습니다. 중복 조사 결과를 보내지 않으려면 Security Hub CSPM에 대해 정의한 규칙을 평가하여 Security Hub에 대해 정의한 규칙과 중복되는지 확인합니다. 해당하는 경우 Security Hub 규칙으로 대체되는 Security Hub CSPM 규칙을 비활성화합니다.

> **Note**
>
> 가장 좋은 방법은 EventBridge에 액세스할 수 있는 권한이 있는 사용자가 최소 필수 권한을 부여하는 AWS Identity and Access Management 정책을 사용하는지 확인하는 것입니다. 자세한 내용은 EventBridge 사용 설명서의 EventBridge 및 AWS Identity and Access Management를 참조하세요.

## EventBridge 이벤트 유형

Security Hub는 다음과 같은 Amazon EventBridge 이벤트 유형을 사용하여 EventBridge와 통합합니다.

Security Hub의 EventBridge 대시보드에서 모든 이벤트에는 이러한 이벤트 유형이 모두 포함됩니다.

Findings Imported V2

Security Hub는 모든 새로운 조사 결과와 기존 조사 결과의 모든 업데이트를 EventBridge에 Findings Imported V2 이벤트로 자동 전송합니다. 각 Findings Imported V2 이벤트에는 단일 조사 결과가 포함됩니다.

가져온 모든 결과와 `BatchUpdateFindingsV2` 요청을 통해 업데이트된 모든 결과는 Findings Imported V2 이벤트를 트리거합니다.

관리자 계정의 경우, EventBridge의 이벤트 피드에는 관리자 계정과 회원 계정 모두에서 찾은 조사 결과에 대한 이벤트가 포함됩니다.

집계 지역의 이벤트 피드에는 집계 지역 및 연결 지역의 조사 결과에 대한 이벤트가 포함됩니다. 지역 간 조사 결과는 거의 실시간으로 이벤트 피드에 포함됩니다.

조사 결과를 문제 해결 워크플로, 타사 도구, 또는 기타 지원되는 EventBridge 대상으로 자동 라우팅하는 규칙을 정의할 수 있습니다. 조사 결과에 특정 속성 값이 있는 경우에만 규칙을 적용하는 필터가 규칙에 포함될 수 있습니다.

이 방법을 사용하여 모든 조사 결과 또는 특정한 특성이 있는 모든 조사 결과를 자동으로 응답 또는 문제 해결 워크플로우로 보냅니다.

> **Note**
>
> Security Hub와 Security Hub CSPM은 모두 소스의 EventBridge로 조사 결과를 전송합니다`aws.securityhub`. Security Hub CSPM 결과와 관련된 중복 알림을 방지하려면 EventBridge 규칙이 Security Hub에 고유한 세부 정보 유형을 사용해야 합니다.

## EventBridge 이벤트 형식

Findings Imported V2 이벤트 유형은 다음 이벤트 형식을 사용합니다.

예제

이 형식은 Security Hub가 EventBridge로 이벤트를 전송할 때 사용됩니다.

```
{
   "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>
       }]
   }
}
```

각 이벤트는 단일 조사 결과를 전송합니다. *<finding content>*는 이벤트에서 전송한 조사 결과의 JSON 형식 내용입니다.

조사 결과 속성의 전체 목록은 Security Hub CSPM의 OCSF 조사 결과를 참조하세요.

## EventBridge에 대한 규칙 구성

Amazon EventBridge에서 Findings Imported V2 이벤트를 수신할 때 수행할 작업을 정의하는 규칙을 생성할 수 있습니다. Findings Imported V2 이벤트는 `BatchUpdateFindingsV2`를 통한 업데이트에 의해 트리거됩니다.

각 규칙에는 규칙을 트리거하는 이벤트를 식별하는 이벤트 패턴이 포함되어 있습니다. 이벤트 패턴에는 항상 이벤트 소스(`aws.securityhub`)와 이벤트 유형(Findings Imported V2)이 포함됩니다. 이벤트 패턴은 규칙이 적용되는 조사 결과를 식별하는 필터를 지정할 수도 있습니다.

그러면 이벤트 규칙이 규칙 대상을 식별합니다. 대상은 EventBridge가 Findings Imported V2 이벤트를 수신하고 조사 결과가 필터와 일치할 때 취할 조치입니다.

여기에 제공된 지침은 EventBridge 콘솔을 사용합니다. 콘솔을 사용하면 EventBridge는 EventBridge가 Amazon CloudWatch Logs에 기록을 활성화할 수 있도록 필요한 리소스 기반 정책을 자동으로 생성합니다.

또한 EventBridge API의 `PutRule` 작업을 사용할 수도 있습니다. 하지만 EventBridge API를 사용하는 경우, 리소스 기반 정책을 생성해야 합니다. 필수 정책에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 CloudWatch Logs 권한을 참조하세요.

### 이벤트 패턴 형식

Findings Imported V2 이벤트의 이벤트 패턴 형식은 다음과 같습니다.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Findings Imported V2"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`은(는) Security Hub를 이벤트를 생성하는 서비스로 식별합니다.
- `detail-type`은(는) 이벤트 유형을 식별합니다.

- `detail`은(는) 선택 사항이며 이벤트 패턴에 대한 필터 값을 제공합니다. 이벤트 패턴에 `detail` 필드가 없는 경우, 모든 조사 결과가 규칙을 트리거합니다.

모든 조사 결과 속성을 기준으로 조사 결과를 필터링할 수 있습니다. 각 값에 대해 하나 이상의 값을 쉼표로 구분한 배열을 제공합니다.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

속성에 둘 이상의 값을 제공하면 해당 값이 `OR`로 결합됩니다. 조사 결과에 나열된 값 중 하나라도 있는 경우, 조사 결과는 개별 속성의 필터와 일치합니다. 예를 들어, `INFORMATIONAL`과 `LOW`를 모두 `Severity.Label` 값으로 제공하면 심각도 레이블이 `INFORMATIONAL` 또는 `LOW`일 경우, 조사 결과가 일치합니다.

속성은 `AND`로 결합됩니다. 제공된 모든 속성에 대한 필터 기준과 일치하면 조사 결과가 일치합니다.

속성 값을 제공할 때는 AWS Open Cybersecurity Schema Framework(OCSF) 구조 내에서 해당 속성의 위치를 반영해야 합니다.

다음 예제에서 이벤트 패턴은 `ProductArn` 및 `Severity.Label`에 대한 필터 값을 제공하므로 Amazon Inspector에서 생성되고 심각도 레이블이 `INFORMATIONAL` 또는 `LOW`인 경우, 조사 결과가 일치합니다.

```
{
    "source": [
        "aws.securityhub"
     ],
    "detail-type": [
        "Findings Imported V2"
    ],
    "detail": {
        "findings": {
            "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
            "Severity": {
                "Label": ["INFORMATIONAL", "LOW"]
            }
        }
    }
}
```

### 이벤트 규칙 생성

사전 정의된 이벤트 패턴 또는 사용자 지정 이벤트 패턴을 사용하여 EventBridge에서 규칙을 생성할 수 있습니다. 사전 정의된 패턴을 선택하면 EventBridge가 자동으로 `source` 및 `detail-type`을 채웁니다. EventBridge는 다음과 같은 조사 결과 속성에 대한 필터 값을 지정하는 필드도 제공합니다.

- `cloud.account.uid`
- `compliance.status`
- `metadata.product.name`
- `resources.uid`
- `severity`
- `status`

#### EventBridge 규칙 생성(콘솔)

1. Amazon EventBridge 콘솔(https://console.aws.amazon.com/events/)을 엽니다.
2. 다음 값을 사용하여 조사 결과 이벤트를 모니터링하는 EventBridge 규칙을 생성합니다.
   - 규칙 유형에서 이벤트 패턴이 있는 규칙을 생성합니다.
   - 이벤트 패턴 작성 방법을 선택합니다.

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
|---|---|---|
| 템플릿 | 이벤트 패턴 섹션에서 다음을 선택합니다.<br>• 이벤트 소스에서 AWS 서비스를 선택합니다.<br>• AWS 서비스에 대해 Security Hub를 선택합니다.<br>• 이벤트 유형에서 Findings Imported V2를 선택합니다. | |

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
| --- | --- | --- |
| | • (선택 사항)규칙을 더 구체적으로 만들려면 필터 값을 추가합니다. 예를 들어, 규칙을 활성 레코드 상태의 조사 결과로 제한하려면 특정 레코드 상태에 대해 활성을 선택합니다. | |

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
|---|---|---|
| 사용자 지정 이벤트 패턴입니다.<br><br>(EventBridge 콘솔에 표시되지 않은 속성을 기반으로 조사 결과를 필터링하려면 사용자 지정 패턴을 사용하세요.) | • 이벤트 패턴 섹션에서 사용자 지정 패턴(JSON 편집기)를 선택하고 다음 이벤트 패턴을 텍스트 영역에 붙여 넣습니다.<br><br>`{ "source": [ "aws.securityhub" ], "detail-type": [ "Findings Imported V2" ], "detail": { "findings": { "<attribute name>": [ "<value1>", "<value2>"] } } }`<br><br>• 필터로 사용할 속성 및 속성 값을 포함하도록 이벤트 패턴을 업데이트합니다.<br><br>예를 들어, 심각도가 `Critical`인 조사 결과에 규칙을 적용하려면 다음 패턴 예제를 사용합니다.<br><br>`{` | |

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
|---|---|---|
| | <pre>"source": ["aws.securityhub" ], "detail-type": ["Findings Imported V2"], "detail":{ "findings": { "Severity": ["Critical"] } } }</pre> | |

- 대상 유형에서 AWS 서비스를 선택하고 대상 선택에서 Amazon SNS 주제 또는 AWS Lambda 함수와 같은 대상을 선택합니다. 규칙에 정의된 이벤트 패턴과 일치하는 이벤트를 수신할 때 대상이 트리거됩니다.

규칙 생성에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 이벤트에 대응하는 Amazon EventBridge 규칙 생성를 참조하세요.

> **Note**
>
> Security Hub CSPM의 결과에 대해 EventBridge 규칙이 정의된 경우 규칙이 Security Hub에 대해 정의된 규칙과 겹칠 수 있습니다. 중복 조사 결과를 보내지 않으려면 Security Hub CSPM에 대해 정의한 규칙을 평가하여 Security Hub에 대해 정의한 규칙과 중복되는지 확인합니다. 해당하는 경우 Security Hub 규칙으로 대체되는 Security Hub CSPM 규칙을 비활성화합니다.

# Security Hub의 서드 파티 통합

AWS Security Hub의 타사 통합을 통해 보안 태세를 강화할 수 있습니다. 이 기능을 사용하면 Security Hub의 조사 결과를 소비하는 통합을 활성화하여 운영, 조사 및 대응 도구를 Security Hub와 통합할 수 있습니다. 현재 Security Hub는 Jira Cloud 및 ServiceNow와의 통합을 지원합니다.

주제


- AWS Security Hub 통합 Jira Cloud
- ServiceNow 통합
- Security Hub 티켓팅 통합을 위한 KMS 키 정책
- 구성된 티켓팅 통합 테스트


# AWS Security Hub 통합 Jira Cloud

이 주제에서는 Security Hub를와 통합하는 방법을 설명합니다Jira Cloud. 이 주제의 절차를 완료하려면 먼저 Jira Cloud 구독 플랜을 구매해야 합니다. 구독 플랜에 대한 자세한 내용은 Atlassian 웹 사이트의 요금을 참조하세요.

이 통합을 통해 Security Hub 조사 결과를 Jira Cloud로 수동 또는 자동으로 전송할 수 있으므로 운영 워크플로의 일부로 관리할 수 있습니다. 예를 들어 조사 및 해결이 필요한 이슈에 소유권을 할당할 수 있습니다.

조직 내 계정의 경우 위임된 관리자만 통합을 구성할 수 있습니다. 위임된 관리자는 모든 멤버 계정 조사 결과에 대해 티켓 생성 기능을 수동으로 사용할 수 있습니다. 또한 위임된 관리자는 자동화 규칙을 사용하여 멤버 계정과 연결된 모든 결과에 대한 티켓을 자동으로 생성할 수 있습니다. 자동화 규칙을 정의할 때 위임된 관리자는 모든 멤버 계정 또는 특정 멤버 계정을 포함할 수 있는 기준을 설정할 수 있습니다. 위임된 관리자를 설정하는 방법에 대한 자세한 내용은 Security Hub에서 위임된 관리자 계정 설정을 참조하세요.

조직에 속하지 않은 계정의 경우 이 기능의 모든 측면을 사용할 수 있습니다.

## 사전 조건

Security Hub를 Jira Cloud 환경에 연결하기 전에 Jira 환경에서 다음 구성 단계를 수행해야 합니다.

- AWS Security Hub for Jira 클라우드 앱을 설치합니다.
- 회사 관리형 소프트웨어 개발 프로젝트가 하나 이상 있어야 합니다.
- Security Hub에서 조사 결과를 수신하려는 소프트웨어 개발 프로젝트에 AWS 앱을 할당합니다.

이러한 각 사전 조건의 단계는 아래에 나열되어 있습니다.

1. Jira Cloud 앱용 AWS Security Hub 설치

Security Hub에는 Jira와의 통합을 지원하는 앱이 있습니다. 이 앱은 사용자 지정 필드와 사용자 지정 문제 유형을 설치합니다. Security Hub는 이를 사용하여 결과에 대한 특정 속성을 채웁니다.

1. Atlassian 사이트에 관리자로 로그인합니다.
2. 설정을 선택하고 앱을 선택합니다.
3. 마켓플레이스 페이지로 이동하면 새 앱 찾기를 선택합니다. 앱 페이지로 이동하면 앱 탐색을 선택한 다음 AWS Security Hub for Jira Cloud를 검색합니다. 그런 다음 지금 가져오기를 선택합니다.

2. 프로젝트 생성 또는 기존 프로젝트 확인

프로젝트를 생성하지 않은 경우 이 단계가 필요합니다. 프로젝트를 생성하는 방법에 대한 자세한 내용은 Jira Cloud Support 설명서의 새 프로젝트 생성을 참조하세요.

프로젝트 생성 요구 사항

새 프로젝트를 생성할 때 다음을 수행해야 합니다.

- 프로젝트 템플릿에 소프트웨어 개발을 선택합니다.
- 프로젝트 유형에 회사 관리형을 선택합니다.

기존 프로젝트의 요구 사항

Security Hub와 통합된 Jira 환경의 모든 기존 프로젝트는 회사 관리형 프로젝트 유형이어야 합니다.

3. Jira Cloud 앱을 위한 AWS Security Hub에 프로젝트 추가

Security Hub가 조사 결과를 Jira 환경에 성공적으로 전송할 수 있으려면 Security Hub와 함께 사용하려는 각 프로젝트가 Jira Cloud 앱용 AWS Security Hub와 연결되어 있어야 합니다. Jira 프로젝트를 앱과 연결하면 Security Hub에 필요한 사용자 지정 필드가 프로젝트와 연결되고 Security Hub가 결과를 프로젝트에 전송할 때 채워질 수 있습니다.

1. Atlassian 사이트에 관리자로 로그인합니다.
2. 설정을 선택하고 앱을 선택합니다.
3. 앱 목록에서 AWS Security Hub for Jira Cloud를 선택합니다.
4. 커넥터 설정 탭을 선택합니다.
5. 활성화된 프로젝트에서 Jira 프로젝트 추가를 선택합니다.

a. 드롭다운에서 모두 추가를 선택하거나 프로젝트를 선택합니다. 전체 프로젝트가 아니라 2개 이상의 프로젝트를 추가하려면 단계의 이 부분을 반복합니다.

b. 저장을 선택합니다.

설치 관리자 탭에서 성공적으로 설치된 프로젝트를 확인할 수 있습니다. 설치 관리자 탭에서 필드, 화면, 상태, 워크플로에 대한 구성을 확인할 수도 있습니다.

Jira Cloud에 대한 자세한 내용은 Atlassian 웹 사이트의 Jira Cloud 리소스를 참조하세요.

## 권장 사항

Jira 환경을 위한 전용 시스템 계정 생성

Security Hub와의 통합은 Jira 인스턴스 내의 특정 사용자와 연결된 OAuth 연결을 Jira Cloud 사용합니다. Security Hub OAuth 연결에 사용할 전용 시스템 계정을 생성하는 것은 다음과 같은 이유로 연결에 권장됩니다.

- 전용 시스템 사용자는 연결이 시간이 지남에 따라 Jira 환경에 대한 권한이 변경될 수 있는 직원과 연결되지 않도록 하여 Security Hub가 Jira 환경과 통합하는 기능에 영향을 미칩니다.
- Security Hub가 Jira에서 생성하는 각 문제에는 OAuth 연결을 생성하는 데 사용된 사용자 이름이 포함된 생성자 필드가 표시됩니다. OAuth 연결에 시스템 계정을 사용하면이 시스템 계정이 티켓 생성자로 표시되므로 다른 Jira 사용자가 수동으로 생성하지 않고 Security Hub 통합을 통해 조사 결과가 생성되었음을 확인할 수 있습니다.

## Security Hub와 간의 통합 구성 Jira Cloud

Security Hub 조사 결과를 보내려는 각 Jira Cloud 프로젝트에 대해 다음 절차를 완료해야 합니다.

> **Note**
>
> Jira Cloud 커넥터를 생성하면 현재에서 AWS 리전 로 리디렉션`"https://3rdp.oauth.console.api.aws"`되므로 커넥터 등록을 완료할 수 있습니다. 그런 다음 커넥터가 생성되는 AWS 리전 로 돌아갑니다.

Jira Cloud 통합을 구성하려면

1. 자격 증명으로 AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 여시겠습니까?region=us-east-1.
2. 탐색 창에서 관리를 선택한 다음 통합을 선택합니다.
3. 추가Jira Cloud를 선택합니다.
4. 세부 정보에 통합의 고유한 설명 이름을 입력하고 통합에 대한 선택적 설명을 입력할지 여부를 결정합니다.
5. 암호화에서 Security Hub 내에서 통합 자격 증명을 암호화하는 방법을 선택합니다.

   - AWS 소유 키 사용 -이 옵션을 사용하면 Security Hub 소유 서비스 키를 사용하여 Security Hub 내에서 통합 자격 증명 데이터를 암호화합니다.
   - 다른 KMS 키(고급) 선택 -이 옵션을 사용하면 Security Hub 내에서 통합 자격 증명 데이터를 암호화하는 데 사용할 AWS KMS key 생성한를 선택합니다. AWS KMS 키 생성 방법에 대한 자세한 내용은  AWS Key Management Service 개발자 안내서의 AWS KMS 키 생성을 참조하세요. 자체 키를 사용하기로 선택한 경우 Security Hub가 키에 액세스할 수 있도록 허용하는 정책 설명을 KMS 키에 추가해야 합니다. 필요한 AWS KMS 정책에 대한 자세한 내용은 Security Hub 티켓팅 통합의 키 정책을 참조하세요.

   > **Note**
   >
   > 이 구성을 완료한 후에는 이러한 설정을 변경할 수 없습니다. 하지만 사용자 지정 키를 선택한 경우 언제든지 사용자 지정 키 정책을 편집할 수 있습니다.

6. (선택 사항) 태그에서 태그를 생성하고 통합에 추가합니다. 최대 50개의 태그를 추가할 수 있습니다.
7. 권한 부여에서 커넥터 생성 및 권한 부여를 선택합니다. 팝업이 나타나면 허용을 선택하여 권한 부여를 완료합니다. 권한 부여를 완료하면 권한 부여가 성공했음을 알리는 확인란이 나타납니다.
8. 구성에 Jira Cloud 프로젝트 ID를 입력합니다.
9. 구성 완료를 선택합니다. 구성을 완료하면 구성된 통합 탭에서 구성된 통합을 볼 수 있습니다.

Jira와의 통합을 구성한 후 연결을 테스트하여 모든 것이 Jira 환경 및 Security Hub에서 올바르게 구성되었는지 확인할 수 있습니다. 자세한 내용은 구성된 티켓팅 통합 테스트를 참조하세요.

## 추가 Jira 통합 세부 정보

### 속도 제한 고려 사항

Jira는 API 속도 제한을 적용하여 서비스 안정성을 유지하고 플랫폼 전체에서 공정한 사용을 보장합니다. AWS Security Hub와 Jira 통합을 사용할 때 이러한 속도 제한은 Security Hub 조사 결과 처리, 특히 대량의 조사 결과를 생성하는 환경에 영향을 미칠 수 있습니다. 이로 인해 티켓 생성이 지연될 수 있으며, 조사 결과 볼륨이 매우 많은 시나리오에서는 일부 조사 결과가 Jira 티켓으로 전혀 처리되지 않을 수 있습니다. 통합을 최적화하려면 Security Hub의 자동화 규칙에 필터를 구현하여 가장 중요한 결과에 대한 티켓팅의 우선순위를 지정하고, 관리자 콘솔을 통해 Jira API 사용량을 모니터링하고, Jira 라이선스 계층의 특정 속도 제한을 기반으로 워크플로를 계획하는 것이 좋습니다. 비즈니스 크리티컬 구현의 경우 Jira 관리자에게 문의하여 속도 제한 할당을 검토하세요.

Jira API 속도 제한에 대한 자세한 내용은 Atlassian 개발자 안내서 웹 사이트의 속도 제한 설명서를 참조하세요.

### 인증 및 보안

Jira API 인증에는 보안 액세스를 위한 적절한 OAuth 2.0 구성이 필요합니다. 애플리케이션이 API 통합에 대한 Atlassian의 보안 모범 사례를 따르는지 확인합니다.

리소스:

- Atlassian 웹 사이트의 Jira REST API v3: Jira REST API v3 설명서
- OAuth 2.0(3LO) 구현: Atlassian 웹 사이트의 OAuth 2.0(3LO) 구현 가이드
- Jira Cloud 앱 관리: Atlassian 웹 사이트의 Jira Cloud 관리 리소스
- Jira 권한 관리: Atlassian 웹 사이트에서 프로젝트 권한 관리

## Jira Cloud 통합에 대한 티켓 생성

Jira Cloud와의 통합을 생성한 후 조사 결과에 대한 티켓을 생성할 수 있습니다.

> **Note**
>
> 조사 결과는 전체 수명 주기 동안 항상 단일 티켓과 연결됩니다. Security Hub는 초기 생성 후 모든 후속 업데이트를 동일한 티켓으로 조사 결과에 전송합니다. 자동화 규칙과 연결된 커넥터가 변경되면 업데이트된 커넥터는 규칙 기준과 일치하는 신규 및 수신 조사 결과에만 사용됩니다.

조사 결과에 대한 티켓을 생성하려면

1. 자격 증명으로 AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.region=us-east-1입니다.
2. 탐색 창의 인벤토리에서 조사 결과를 선택합니다.
3. 조사 결과를 선택합니다. 조사 결과에서 티켓 생성을 선택합니다.
4. 통합에서 드롭다운 메뉴를 열고 통합을 선택합니다. 이 통합은 이전에 Jira Cloud 프로젝트를 구성할 때 생성한 통합입니다. 조사 결과를 전송할 통합을 선택합니다.
5. 생성(Create)을 선택합니다.

### Jira Cloud 통합에 대한 티켓 보기

조사 결과에 대한 티켓을 생성한 후 Jira Cloud 인스턴스에서 티켓을 열 수 있습니다.

Jira Cloud 인스턴스에서 조사 결과를 보려면

1. 자격 증명으로 AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.region=us-east-1입니다.
2. 탐색 창의 인벤토리에서 조사 결과를 선택합니다.
3. 티켓을 생성한 조사 결과를 선택합니다.
4. 조사 결과에서 티켓 ID를 선택하여 Jira Cloud 인스턴스에서 티켓을 보거나 JSON 보기를 선택합니다.

## ServiceNow 통합

이 주제에서는 Security Hub 콘솔에 액세스하여 ServiceNow ITSM 통합을 구성하는 방법을 설명합니다. 이 주제의 절차를 완료하기 전에 ServiceNow ITSM 구독이 있어야 이 통합을 추가할 수 있습니다. 자세한 내용은 ServiceNow 웹사이트의 요금 페이지를 참조하세요.

조직 내 계정의 경우 위임된 관리자만 통합을 구성할 수 있습니다. 위임된 관리자는 모든 멤버 계정 조사 결과에 대해 티켓 생성 기능을 수동으로 사용할 수 있습니다. 또한 위임된 관리자는 자동화 규칙을 사용하여 멤버 계정과 연결된 모든 결과에 대한 티켓을 자동으로 생성할 수 있습니다. 자동화 규칙을 정의할 때 위임된 관리자는 모든 멤버 계정 또는 특정 멤버 계정을 포함할 수 있는 기준을 설정할 수 있습니다. 위임된 관리자를 설정하는 방법에 대한 자세한 내용은 Security Hub에서 위임된 관리자 계정 설정을 참조하세요.

조직에 속하지 않은 계정의 경우 이 기능의 모든 측면을 사용할 수 있습니다.

## 사전 조건 - ServiceNow 환경 구성

ServiceNow ITSM 통합을 구성하기 전에 다음 사전 조건을 완료해야 합니다. 그렇지 않으면 ServiceNow ITSM와 Security Hub 간의 통합이 작동하지 않습니다.

1. IT Service Management(ITSM)에 대한 Security Hub 조사 결과 통합 설치

다음 절차에서는 Security Hub 플러그인을 설치하는 방법을 설명합니다.

1. ServiceNow ITSM 인스턴스에 로그인한 다음 애플리케이션 탐색기를 엽니다.
2. ServiceNow 스토어로 이동합니다.
3. IT Service Management(ITSM)에 대한 Security Hub 조사 결과 통합을 검색한 다음 가져오기를 선택하여 애플리케이션을 설치합니다.

> **Note**
>
> Security Hub 애플리케이션의 설정에서 새 Security Hub 조사 결과가 ServiceNow ITSM 환경으로 전송될 때 수행할 작업을 선택합니다. 아무 작업 안함, 인시던트 생성, 문제 생성 또는 둘 다 생성(인시던트/문제)을 선택할 수 있습니다.

2. 인바운드 OAuth 요청에 대한 클라이언트 자격 증명 권한 부여 유형 구성

인바운드 OAuth 요청에 대해 이 권한 부여 유형을 구성해야 합니다. 자세한 내용은 ServiceNow Support 웹 페이지에서 Client Credentials grant type for Inbound OAuth is supported를 참조하세요.

3. OAuth 애플리케이션 생성

OAuth 애플리케이션을 이미 생성한 경우 이 사전 조건을 건너뛸 수 있습니다. OAuth 애플리케이션 생성에 대한 자세한 내용은 ServiceNow 웹 사이트의 OAuth 설정을 참조하세요.

## 사전 조건 - 구성 AWS Secrets Manager

Security Hub와 ServiceNow의 통합을 사용하려면 ServiceNow OAuth 애플리케이션의 자격 증명을 Secrets Manager에 저장해야 합니다. Secrets Manager에 자격 증명을 저장하면 자격 증명 사용에 대한 제어 및 가시성을 확보하는 동시에 Security Hub가 자격 증명을 사용하여 ServiceNow 인스턴스와 통합할 수 있습니다. Secrets Manager에 자격 증명을 저장하려면 고객 관리형 AWS KMS 키를 사용하여 보안 암호를 보호해야 합니다. 이 AWS KMS 키를 사용하면 저장 시 보안 암호를 보호할 수 있으며

보안 암호를 보호하는 키에 액세스할 수 있는 권한을 Security Hub에 부여하는 정책을 키에 연결할 수도 있습니다.

다음 단계에 따라 ServiceNow 자격 증명에 대해 Secrets Manager를 구성합니다.

1단계: AWS KMS 키에 정책 연결

ServiceNow 통합을 성공적으로 구성하려면 먼저 Secrets Manager에서 ServiceNow 자격 증명과 연결된 AWS KMS 키를 사용할 수 있는 권한을 Security Hub에 부여해야 합니다.

Security Hub가 ServiceNow 자격 증명에 액세스하도록 AWS KMS 키 정책을 수정하려면

1. https://console.aws.amazon.com/kms AWS KMS 콘솔을 엽니다.
2. AWS 리전을 변경하려면 페이지 오른쪽 상단에 있는 리전 선택기를 사용합니다.
3. 기존 AWS KMS 키를 선택하거나 AWS KMS 개발자 안내서의 새 키 생성 단계를 수행합니다.
4. 키 정책 섹션에서 편집을 선택합니다.
5. 정책 보기로 전환이 표시되면 이를 선택하여 키 정책을 표시한 다음 편집을 선택합니다.
6. 다음 정책 블록을 AWS KMS 키 정책에 복사하여 Security Hub에 키를 사용할 수 있는 권한을 부여합니다.

```
{
    "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. 정책 예제에서 다음 값을 대체하여 정책을 편집합니다.
   - *your-account-id*를 AWS 계정 ID로 바꿉니다.
   - *your-region*을 AWS 해당 리전(예: us-east-1)으로 바꿉니다.
8. 최종 문 앞에 정책 문구를 추가한 경우 이 문구를 추가하기 전에 쉼표를 추가합니다. AWS KMS 키 정책의 JSON 구문이 유효한지 확인합니다.
9. 저장을 선택합니다.
10. (선택 사항) 이후 단계에서 사용할 수 있도록 키 ARN을 메모장에 복사합니다.

### 2단계: Secrets Manager에서 보안 암호 생성

Secrets Manager에서 ServiceNow 보안 인증 정보를 저장할 보안 암호를 생성합니다. Security Hub는 ServiceNow 환경과 상호 작용할 때이 보안 암호에 액세스합니다.

AWS Secrets Manager 사용 설명서의 보안 암호 생성 단계를 따릅니다. 보안 암호를 생성한 후 Security Hub 커넥터를 생성할 때 필요하므로 보안 암호 ARN을 복사합니다.

보안 암호를 생성할 때 다음을 구성해야 합니다.

보안 암호 유형

다른 유형의 보안 암호

키/값 페어(일반 텍스트 형식)

```
{
    "ClientId": "your-servicenow-client-id",
    "ClientSecret": "your-servicenow-client-secret"
```

```
    }
```

> **Note**
>
> 필드 이름은 정확히 `ClientId` 및 `ClientSecret` (대/소문자 구분)여야 합니다. Security Hub에서 자격 증명을 검색하려면 이러한 정확한 이름이 필요합니다.

암호화 키

1단계에서 구성한 AWS KMS 키 사용

리소스 정책

다음 리소스 정책을 사용합니다.

```
{
    "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:*"
            }
        }
        }
    ]
    }
```

이제 보안 암호가 구성되었으므로 CreateConnectorV2 API 또는 AWS 콘솔을 사용하여 Security Hub 커넥터를 생성할 수 있습니다. 다음을 제공해야 합니다.

- InstanceName: ServiceNow 인스턴스 URL(예: `your-instance.service-now.com`)

- SecretArn:이 절차에서 생성한 보안 암호의 ARN

## ServiceNow ITSM 통합 구성

Security Hub는 ServiceNow ITSM에서 인시던트 또는 문제를 자동으로 생성할 수 있습니다.

ServiceNow ITSM 통합을 구성하려면

1. 자격 증명으로 AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 여시겠습니까?region=us-east-1입니다.
2. 탐색 창에서 관리를 선택한 다음 통합을 선택합니다.
3. ServiceNow ITSM에서 통합 추가를 선택합니다.
4. 세부 정보에 통합의 을 입력하고 통합에 대한 선택적 설명을 입력할지 여부를 결정합니다.
5. 암호화에서 Security Hub 내에서 통합 자격 증명을 암호화하는 방법을 선택합니다.

   - AWS 소유 키 사용 -이 옵션을 사용하면 Security Hub 소유 서비스 키를 사용하여 Security Hub 내에서 통합 자격 증명 데이터를 암호화합니다.
   - 다른 KMS 키(고급) 선택 -이 옵션을 사용하면 Security Hub 내에서 통합 자격 증명 데이터를 암호화하는 데 사용할 AWS KMS key 생성한를 선택합니다. AWS KMS 키 생성 방법에 대한 자세한 내용은  AWS Key Management Service 개발자 안내서의 AWS KMS 키 생성을 참조하세요. 자체 키를 사용하기로 선택한 경우 Security Hub가 키에 액세스할 수 있도록 허용하는 정책 설명을 KMS 키에 추가해야 합니다. 필요한 AWS KMS 정책에 대한 자세한 내용은 Security Hub 티켓팅 통합의 키 정책을 참조하세요.

   > **Note**
   >
   > 이 구성을 완료한 후에는 이러한 설정을 변경할 수 없습니다. 하지만 사용자 지정 키를 선택한 경우 언제든지 사용자 지정 키 정책을 편집할 수 있습니다.

6. 자격 증명에 ServiceNow ITSM URL과 사전 조건 섹션에서 생성된 AWS Secrets Manager 보안 암호의 ARN을 입력합니다.
7. 태그에서 선택적 태그를 생성하고 통합에 추가할지 여부를 결정합니다.
8. 통합 추가(Add Integrations)를 선택합니다. 구성을 완료하면 구성된 통합 탭에서 구성된 통합을 볼 수 있습니다.

ServiceNow와의 통합을 구성한 후 연결을 테스트하여 ServiceNow 환경 및 Security Hub에서 모든 것이 올바르게 구성되었는지 확인할 수 있습니다. 자세한 내용은 구성된 티켓팅 통합 테스트를 참조하세요.

## ServiceNow ITSM 통합에 대한 티켓 생성

ServiceNow ITSM와의 통합을 생성한 후 조사 결과에 대한 티켓을 생성할 수 있습니다.

> **Note**
>
> 조사 결과는 전체 수명 주기 동안 항상 단일 티켓과 연결됩니다. Security Hub는 초기 생성 후 모든 후속 업데이트를 동일한 티켓으로 조사 결과에 전송합니다. 자동화 규칙과 연결된 커넥터가 변경되면 업데이트된 커넥터는 규칙 기준과 일치하는 신규 및 수신 조사 결과에만 사용됩니다.

조사 결과에 대한 티켓을 생성하려면

1. 자격 증명으로 AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.region=us-east-1.
2. 탐색 창의 인벤토리에서 조사 결과를 선택합니다.
3. 조사 결과를 선택합니다. 조사 결과에서 티켓 생성을 선택합니다.
4. 통합에서 드롭다운 메뉴를 열고 통합을 선택합니다.
5. 생성(Create)을 선택합니다.

## ServiceNow ITSM 통합에 대한 티켓 보기

조사 결과에 대한 티켓을 생성한 후 ServiceNow ITSM 인스턴스에서 티켓을 열 수 있습니다.

ServiceNow ITSM 인스턴스에서 조사 결과를 보려면

1. 자격 증명으로 AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.region=us-east-1.
2. 탐색 창의 인벤토리에서 조사 결과를 선택합니다.
3. 티켓을 생성한 조사 결과를 선택합니다.
4. 조사 결과에서 티켓 ID를 선택하여 ServiceNow ITSM 인스턴스에서 티켓을 보거나 JSON 보기를 선택합니다.

# Security Hub 티켓팅 통합을 위한 KMS 키 정책

Security Hub 티켓팅 통합과 함께 고객 관리형 KMS 키를 사용하는 경우 Security Hub가 키와 상호 작용할 수 있도록 KMS 키에 추가 정책을 추가해야 합니다. 또한 키를 Security Hub 커넥터 권한에 추가하는 보안 주체가 키에 액세스할 수 있도록 허용하는 정책을 추가해야 합니다.

## Security Hub 권한 정책

다음 정책은 Security Hub가 Jira 및 ServiceNow 커넥터와 연결된 KMS 키에 액세스하고 사용할 수 있어야 하는 권한을 간략하게 설명합니다. 이 정책은 Security Hub 커넥터와 연결된 각 KMS 키에 추가해야 합니다.

정책에는 다음 권한이 포함됩니다.

- Security Hub가 키를 사용하여 티켓팅 통합과 통신하는 데 사용되는 임시 액세스 또는 새로 고침 토큰을 보호할 수 있도록 허용합니다. 권한은 소스 ARN 및 암호화 컨텍스트를 확인하는 조건 블록을 통해 특정 Security Hub 커넥터와 관련된 작업으로 제한됩니다.
- Security Hub가 `DescribeKey` 작업을 허용하여 KMS 키에 대한 메타데이터를 읽을 수 있도록 허용합니다. 이 권한은 Security Hub가 키의 상태 및 구성을 확인하는 데 필요합니다. 액세스는 소스 ARN 조건을 통해 특정 Security Hub 커넥터로 제한됩니다.

```
{
    "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/*"
        }
    }
}
```

정책 예제에서 다음 값을 대체하여 정책을 편집합니다.

- *CloudProviderName*을 JIRA_CLOUD 또는 로 바꾸기 SERVICENOW
- *AccountId*를 Security Hub 커넥터를 생성하는 계정 ID로 바꿉니다.
- *##*을 해당 AWS 리전으로 바꿉니다(예: us-east-1).

## Security Hub 작업을 위한 IAM 위탁자 액세스

고객 관리형 KMS 키를 Security Hub 커넥터에 할당하는 모든 보안 주체는 커넥터에 추가되는 키에 대한 키 작업(별칭 설명, 생성, 복호화, 재암호화 및 나열)을 수행할 수 있는 권한이 있어야 합니다. 이는 CreateConnectorV2 및 CreateTicketV2 APIs에 적용됩니다. 다음 정책 설명은 이러한 APIs와 상호 작용하는 모든 보안 주체에 대한 정책의 일부로 포함되어야 합니다.

```
{
    "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"
            ]
        }
    }
}
```

정책 예제에서 다음 값을 대체하여 정책을 편집합니다.

- *RoleName*을 Security Hub를 호출하는 IAM 역할의 이름으로 바꿉니다.
- *CloudProviderName*을 JIRA_CLOUD 또는 로 바꿉니다SERVICENOW.
- *AccountId*를 Security Hub 커넥터를 생성하는 계정 ID로 바꿉니다.

- ##을 해당 AWS 리전으로 바꿉니다(예: us-east-1).

## 구성된 티켓팅 통합 테스트

구성된 Jira 및 ServiceNow 통합의 경우 연결을 테스트하여 Security Hub와 Jira 또는 ServiceNow 환경의 모든 구성이 완료되었는지 확인할 수 있습니다.

테스트 티켓 기능은 제목이 인 티켓을 생성합니다TESTING Test CreateTicketV2 Finding. 테스트 티켓은 테스트가 수행되는 계정의 계정 ID 및 리전, 샘플 리소스 세부 정보, 샘플 AWS 결과 JSON과 같은 샘플 데이터로 채워집니다.

### 콘솔을 사용하여 통합 테스트

다음 단계에 따라 통합을 테스트합니다.

1. Security Hub 탐색 패널에서 통합을 선택합니다.
2. 구성된 통합 탭에서 테스트할 통합을 선택했습니다.
3. 통합의 개요 페이지에서 테스트 티켓 생성을 선택합니다.
4. Security Hub는 테스트가 성공하면 성공 메시지와 테스트 티켓에 대한 링크를 표시합니다. 테스트에 실패하면 Security Hub에 오류가 표시됩니다. 오류 메시지에 따라 Security Hub 또는 Jira 또는 ServiceNow 환경에서 구성 문제를 해결합니다.

> **Note**
>
> 새 연결 설정 또는 기존 연결을 변경할 때 엔드 투 엔드 기능을 확인하는 데 도움이 되는 테스트 티켓 기능입니다. 이 기능은 Jira 또는 ServiceNow 환경이 사용될 때마다 새 티켓을 생성하며 연결을 정기적으로 확인하기 위한 것이 아닙니다.

### 를 사용한 테스트 AWS CLI

를 사용하여 통합을 테스트하려면 --mode DRYRUN 파라미터와 함께 create-ticket-v2 명령을 AWS CLI사용합니다.

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
```

```
  --region <your-region> \
  --connector-id <your-connector-id> \
  --finding-metadata-uid "TEST_FINDING"
```

예제

다음 예제에서는 통합을 테스트하는 방법을 보여줍니다.

```
aws securityhub create-ticket-v2 \
  --mode DRYRUN \
  --region us-east-1 \
  --connector-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
  --finding-metadata-uid "TEST_FINDING"
```

응답 성공

응답이 성공하면 다음이 반환됩니다.

```
{
    "TicketId": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6",
    "TicketSrcUrl": "https://your-instance.service-now.com/nav_to.do?
uri=x_aws_se_0_finding.do?sys_id=a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6"
}
```

응답`TicketSrcUrl`의는 Jira 또는 ServiceNow 환경에서 테스트 티켓을 볼 수 있는 직접 링크를 제공합니다.

테스트가 실패하면 해결해야 할 구성 문제를 나타내는 오류 메시지가 표시됩니다.

## Jira 클라우드 통합 오류 문제 해결

Security HubJira Cloud에서에 대한 통합을 테스트할 때 다음 오류 메시지가 반환될 수 있습니다. 이러한 오류 메시지는 커넥터의 구성 문제가 발생할 수 있는 위치와 해결 방법을 파악할 수 있습니다.

Jira Cloud 통합 오류 메시지

| 오류 | 오류 메시지 | 가능한 원인 및 해결 방법 |
| --- | --- | --- |
| ConflictException | 지라 프로젝트를 찾을 수 없음 | 가능한 원인: 커넥터의 프로젝트가 올바르지 않거나 자격 증명/권한 문제로 인해 프로젝트에 액세스할 수 없습니다.<br><br>가능한 해결 방법: 커넥터에 올바른 프로젝트를 추가하거나 올바른 자격 증명을 사용하여 Jira에 다시 인증합니다. |
| ConflictException | Security Hub 문제 유형을 찾을 수 없음 | 가능한 원인: 앱 설치 문제 또는 문제 유형이 프로젝트와 연결되어 있지 않습니다.<br><br>가능한 해결 방법: 사전 조건 단계를 수행하여 Jira 앱을 Jira 환경에 설치하고 앱을 프로젝트와 연결합니다. |

# MCP 앱(미리 보기)

Security Hub는 모델 컨텍스트 프로토콜(MCP) 앱을 통해 에이전트 경험을 제공합니다. 이 앱을 사용하면 AI 에이전트가 노출 조사 결과를 조사할 수 있습니다. 또한 생성 전에 기존 Azure 커넥터를 진단하거나 Azure 커넥터 사전 조건을 평가할 수 있습니다.

각 조사 결과 도구 호출은 에이전트가 추론할 수 있는 텍스트 요약을 반환합니다. 사용 가능한 경우 동일한 대화에서 확인할 수 있는 대화형 시각화도 반환됩니다. Connector Diagnostics는 확인된 조사 결과를 확인할 수 없는 검사 결과와 구분하는 구조화된 텍스트를 반환합니다.

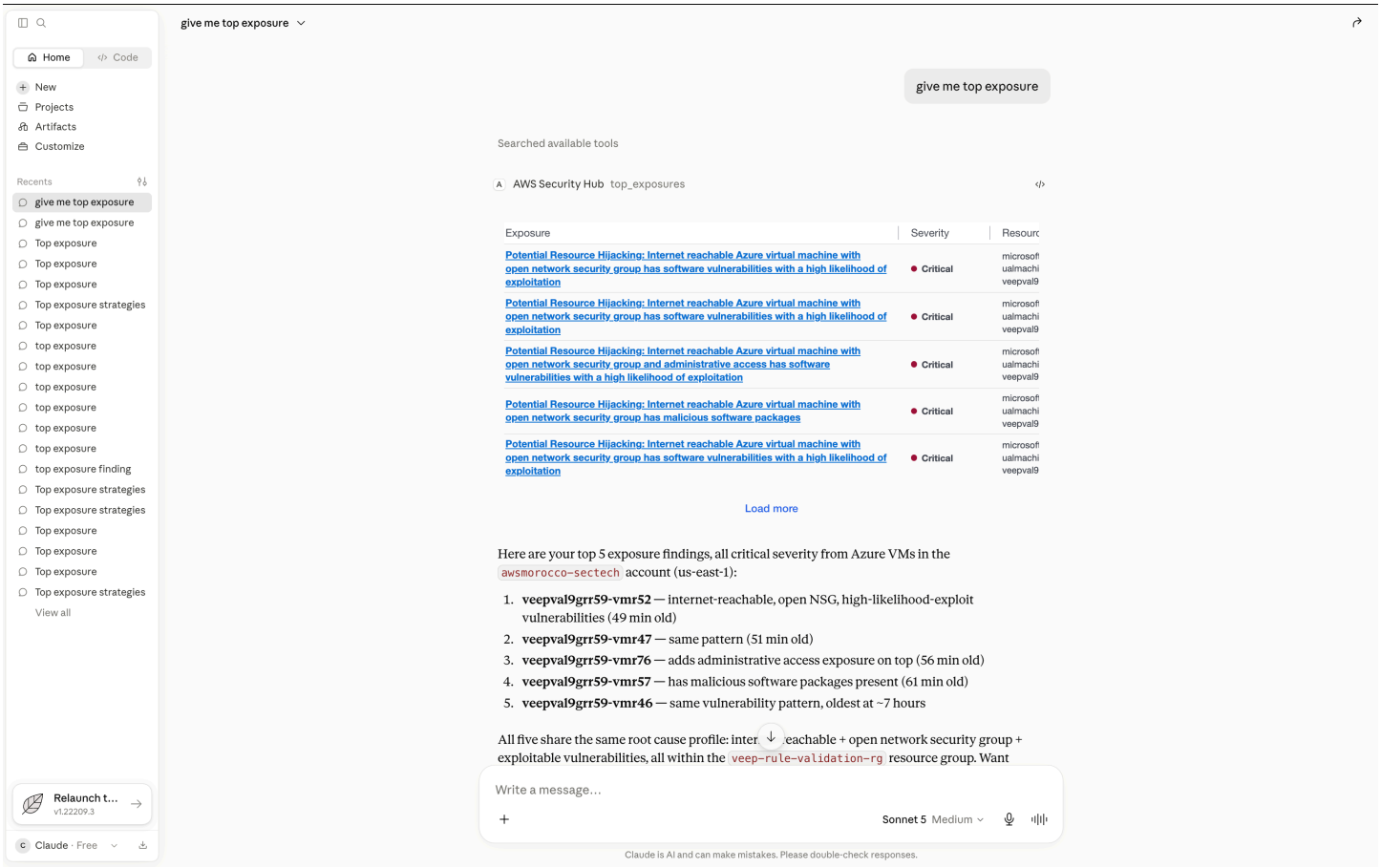
MCP 앱은 시스템에서 실행되고 기존 AWS 자격 증명을 사용하여 Security Hub APIs 직접 호출하는 로컬 MCP 서버입니다. Connector Diagnostics는 기존 Azure CLI 세션을 사용하여 한정된 읽기 전용 Azure CLI 쿼리를 실행할 수도 있습니다. 모든 도구는 읽기 전용이며 보안 태세 또는 커넥터 리소스를 수정하지 않습니다. MCP 앱은 Security Hub를 사용할 수 있는 모든 AWS 상용 리전에서 사용할 수 있습니다.

> **Important**
>
> Security Hub MCP 앱은 공개 미리 보기 상태입니다.

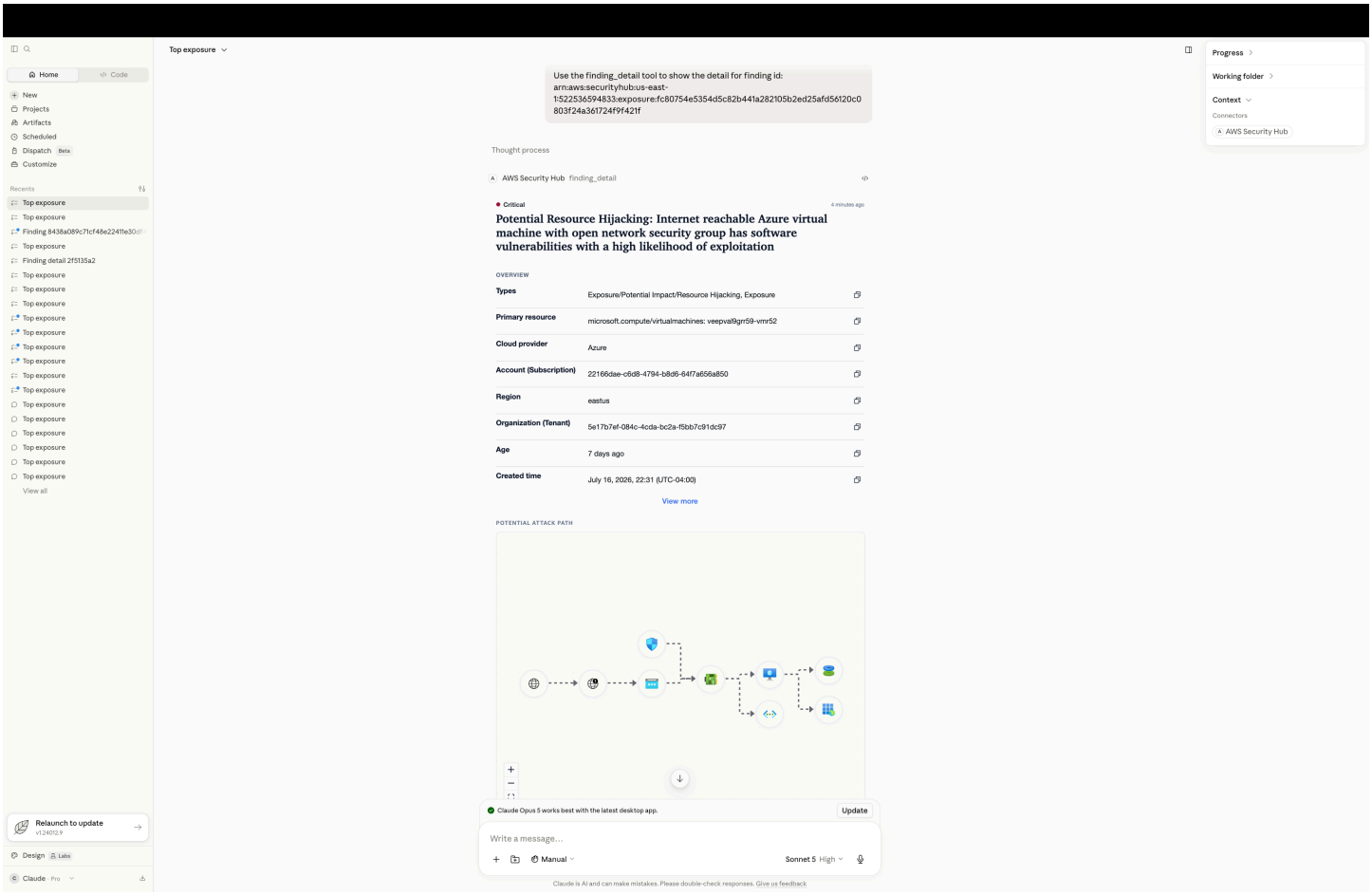
# MCP 앱 예제

다음 예제에서는 노출을 조사하는 동안 MCP 앱이 Claude 데스크톱 내에서 대화형 시각화를 렌더링하는 방법을 보여줍니다.

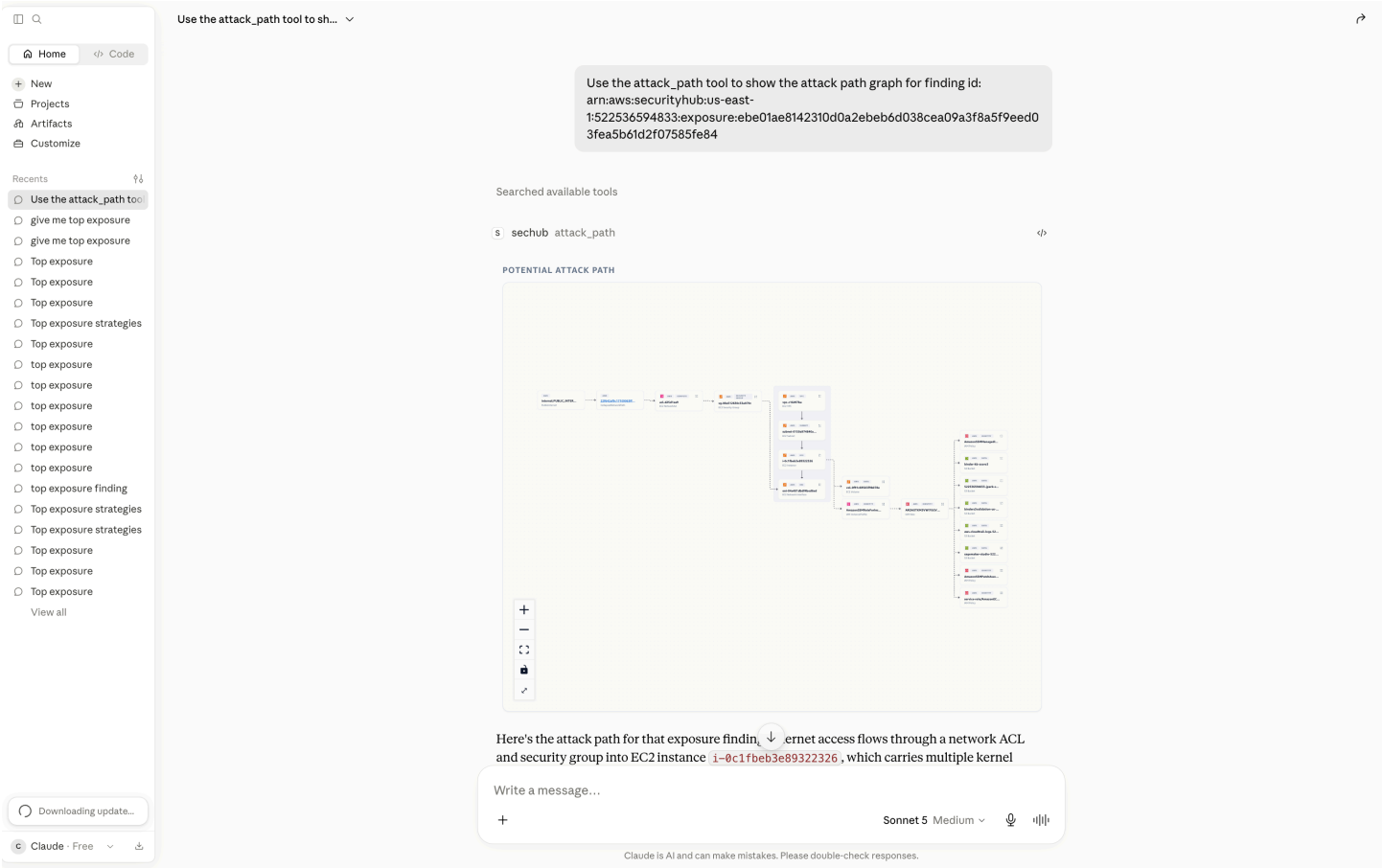
상위 노출 - 대화형 테이블에 가장 중요한 노출 조사 결과를 나열합니다. 다음 이미지는 상위 노출 테이블을 보여줍니다.



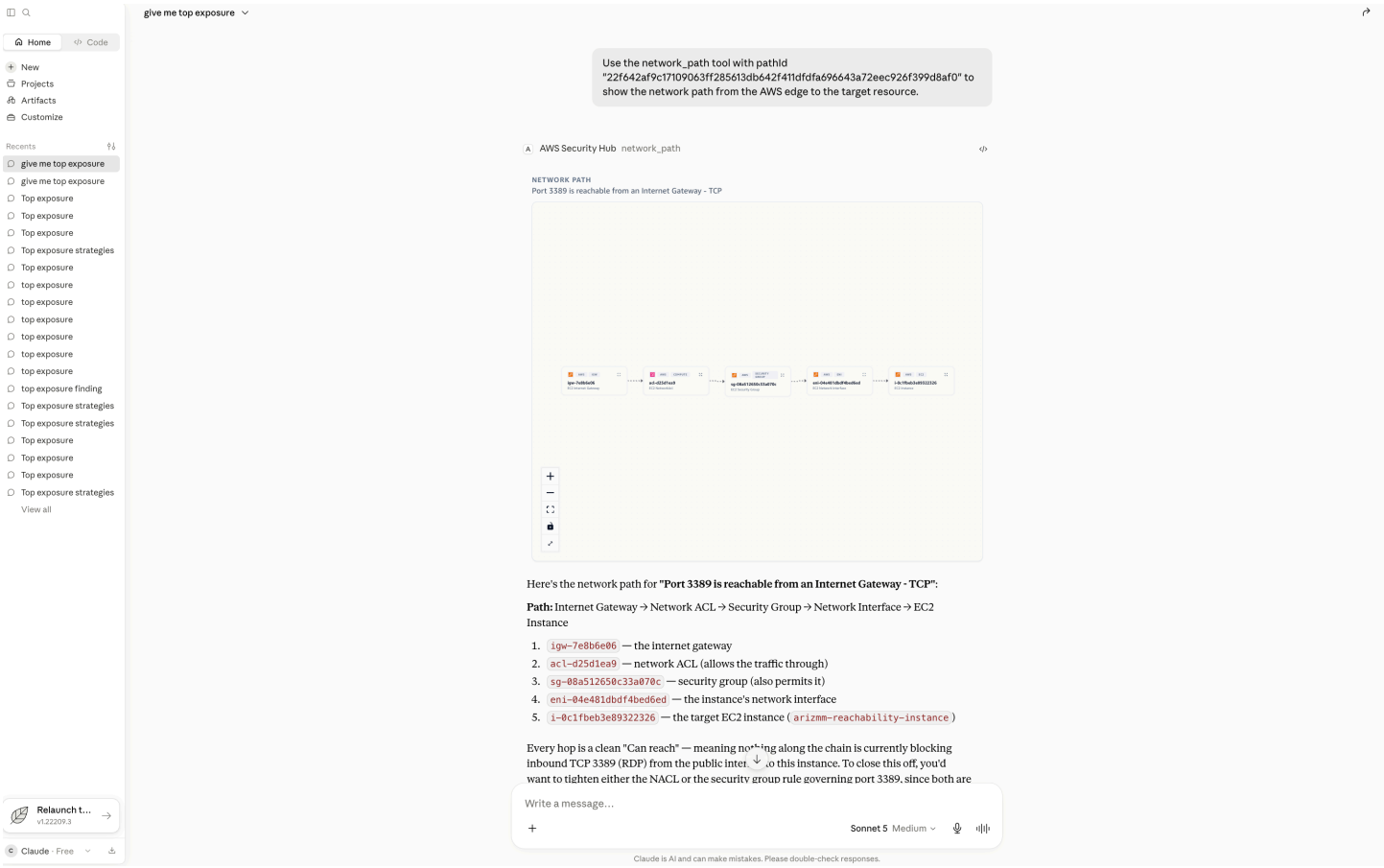

조사 결과 세부 정보 - 상관관계가 있는 조사 결과 특성 요약, 공격 경로 및 문제 해결 지침과 함께 단일 노출 조사 결과의 개요를 검토합니다. 다음 이미지는 결과 세부 정보 보기를 보여줍니다.




공격 경로 - 노출에 도달하는 방법을 대화형 그래프로 시각화합니다. 노드는 리소스, 자격 증명 및 서비스를 나타냅니다. 엣지는 엣지 간의 관계를 나타냅니다. 다음 이미지는 공격 경로 그래프를 보여줍니다.




네트워크 경로 - AWS 엣지에서 대상 리소스로 정렬된 네트워크 홉을 탐색합니다(예: Internet Gateway에서 NACL로, Security Group에서 ENI로, 인스턴스로). 다음 이미지는 네트워크 경로를 보여줍니다.




커넥터 진단 - 기존 Azure 커넥터가 성능 저하되거나 실패한 이유를 질문합니다. 에이전트는 확인된 문제를 식별하고, 확인할 수 없는 검사를 구분하며, 환경을 변경하지 않고 가장 작은 복구를 권장합니다.

커넥터 준비 - 커넥터를 생성하기 전에 Azure 사전 조건을 확인합니다. 에이전트는 통과, 실패 또는 확인할 수 없는 사전 조건을 보고합니다.

## 주요 개념

노출 조사 결과 - 취약성, 잘못된 구성, 네트워크 연결성, 민감한 데이터와 같은 여러 신호를 위험에 노출된 리소스의 단일 보기와 연관시키는 조사 결과입니다.

커넥터 진단 - Azure 커넥터를 위한 세 가지 읽기 전용 도구입니다. 도구는 기존 커넥터를 진단하고, 제안된 설정을 평가하고, 지원되는 Azure 설정 스크립트에서 정확한 발췌문을 검색합니다. 에이전트는 도구를 선택하고 구조화된 결과를 설명으로 변환합니다.

로컬 MCP 서버 - 컴퓨터에서 실행되고 Claude Desktop과 Security Hub 간의 안전한 양방향 브리지 역할을 하는 프로그램입니다. 서버에는 Claude Desktop 내에서 UI를 렌더링하는 도구를 포함하여 AI 에이전트가 사용하는 도구가 포함되어 있습니다. 시스템의 AWS 자격 증명 체인을 사용하며 자체 자격 증명을 보유하지 않습니다.

MCP 앱 - Claude 데스크톱 내에서 렌더링되는 대화형 애플리케이션입니다. 각 MCP 앱 보기는 상위 노출 테이블 또는 공격 경로 그래프 표시와 같은 단일 작업을 수행합니다.

이중 응답 - 단일 조사 결과 도구 호출은 에이전트가 추론하는 간단한 텍스트 요약과 검토할 수 있도록 동일한 대화에서 렌더링된 대화형 시각화라는 두 가지 출력을 반환합니다.

## 사전 조건

- Security Hub가 활성화된 AWS 계정입니다. 노출 조사 결과는 조사 결과 및 노출 도구에만 필요합니다.
- Claude 데스크톱이 설치되었습니다. 설치 관리자는 Claude 웹 사이트에서 Claude 데스크톱 다운로드를 참조하세요.
- AWS 표준 AWS SDK 자격 증명 체인에 구성된 자격 증명입니다.
- Azure 측 커넥터 진단의 경우 Azure CLI를 설치합니다. `az login --tenant ### ID`를 실행하여 커넥터의 테넌트에 인증합니다. 여기서 *### ID*는 커넥터가 포함된 Azure 테넌트의 ID입니다. MCP 앱은 결과 로컬 Azure CLI 세션을 사용합니다. MCP 구성에 Azure 자격 증명을 추가하지 마십시오.

> **Note**
>
> 인증된 Azure CLI 세션 없이 Connector Diagnostics를 실행할 수 있습니다. 결과에는 사용 가능한 AWS측 평가가 포함되며 Azure 종속 검사는 확인되지 않음으로 표시됩니다. 사용할 수 없는 Azure 증거를 정상으로 취급하지 않습니다.

## MCP 서버 설정

MCP 앱은 번들 파일에서 Claude Desktop에 설치합니다. 설치하기 전에 서버가 자격 AWS 증명과 리전을 읽을 수 있도록가 `aws sts get-caller-identity` 성공하고이 터미널에 리전을 `aws configure get region` 반환하는지 확인합니다.

1. Security Hub MCP 앱 번들을 다운로드합니다.
2. 다운로드한 `.mcpb` 파일을 엽니다. Claude Desktop이 구성 흐름을 시작합니다. 지침에 따라 서버를 설치합니다.
3. 연결을 확인하려면 Claude Desktop에 “내 주요 보안 노출 사항은 무엇인가요?”와 같은 질문을 입력합니다. 또는 “ us-west-2의 Azure 커넥터 성능이 저하되었습니다. 무엇이 잘못된지 확인할 수 있나요?” 오류가 발생하면 오류 메시지의 지침을 검토하고 자격 증명과 리전을 확인합니다.

# 커넥터 진단 사용

커넥터 문제 또는 제안된 설정을 자연어로 설명합니다. 에이전트는 적절한 읽기 전용 도구를 선택하고, 구조화된 결과를 해석하고, 확인된 검사와 확인되지 않은 검사를 알려줍니다.

## 기존 커넥터 진단

1. 커넥터 ID 또는 정확한 이름으로 커넥터를 식별합니다. 또한 에이전트가 요청에서 커넥터를 확인할 수 없는 경우 커넥터가 포함된 AWS 계정과 리전을 제공합니다.
2. " us-west-2의 Azure 커넥터 성능이 저하되었습니다. 무엇이 잘못된지 확인하고 먼저 무엇을 수정해야 하는지 알려주실 수 있나요?"
3. 확인되지 않은 점검과 별도로 확인된 결과를 검토합니다. Azure 인증을 사용할 수 없는 경우 에이전트는 결론을 증거 AWS로 제한합니다.

## 제안된 커넥터 평가

1. AWS 계정, AWS 리전 및 Azure 테넌트 ID를 제공합니다. 또한 제안된 커넥터에서 다룰 Azure 구독 IDs 1~10개를 제공합니다. 에이전트에게 평가할 서비스 사전 조건인 클라우드 보안 태세 관리(CSPM), Inspector VM 스캔 또는 위협 탐지를 알립니다. 이러한 선택은 준비 확인의 범위를 지정합니다. 커넥터 생성 설정은 아닙니다.
2. "Azure 커넥터를 생성하기 전에 사전 조건이 이러한 구독에 대해 준비되었는지 확인하세요."와 같은 질문을 합니다.
3. 통과, 실패 및 확인되지 않은 검사를 검토합니다. 정상 준비 결과는 확인된 사전 조건이 통과되었음을 의미합니다. 커넥터가 존재하거나, 실행 중이거나, 복구되었다는 의미는 아닙니다.

## 설정 지침 검색

결과가 온보딩 단계를 참조하는 경우 에이전트에게 해당 단계를 표시하도록 요청합니다. 예를 들어 "지원되는 Azure 커넥터 설정 스크립트의 6단계를 보여줘."라고 질문합니다. 전체 스크립트는 Security Hub와 통합하도록 Microsoft Azure 구성을 참조하세요. 도구는 정확한 발췌문을 반환하지만 실행하지는 않습니다. 단계가 구성 및 헬퍼 함수를 공유하므로 지원되는 전체 스크립트를 실행합니다.

> **Note**
>
> Connector Diagnostics는 리소스를 수리하거나 변경하지 않습니다. 문제 해결은 사용자가 제어하는 별도의 작업에 대한 지침입니다. 진단은 새로운 런타임 증거가 이를 입증할 때만 복구를 보고합니다.

## 사용 가능한 도구

**`top_exposures`** - 가장 긴급한 노출 조사 결과를 대화형 테이블로 나열합니다. 조사 결과당 도구에는 이 목록의 조사 결과 ID가 필요하므로 먼저이 도구를 호출합니다.

**`finding_detail`** - 상관관계가 있는 조사 결과 특성 요약을 포함하여 한 조사 결과의 개요를 반환합니다.

**`finding_overview`** - 결과 ID별로 하나의 결과에 대한 텍스트 요약을 반환합니다.

**`correlated_finding_detail`** - 취약성, 구성 오류 또는 연결 가능성과 같은 단일 특성에 대한 하나의 노출과 상관관계가 있는 결과를 나열합니다.

**`attack_path`** - 하나의 결과에 대한 공격 경로 그래프를 빌드합니다.

**`network_path`** - 결과의 네트워크 경로를 AWS 엣지에서 대상 리소스로 정렬된 홉으로 확장합니다.

**`recommendation`** - 설명서 링크를 포함하여 하나의 결과에 대한 수정 지침을 반환합니다.

**`resource_detail`** - 짧은 ID(예: `i-1234`) 또는 ARN으로 AWS 리소스 하나의 구성을 반환합니다.

**`diagnose_connector`** - 사용 가능한 경우 Security Hub 상태 및 경계 Azure CLI 증거를 사용하여 기존 Azure 커넥터를 진단합니다. 확인된 결과, 영향을 받는 범위, 수정 지침 및 데이터 최신성을 반환합니다. 또한 확인할 수 없는 검사도 나열됩니다.

**`assess_connector_readiness`** - 생성 전에 제안된 Azure 커넥터에 대한 AWS측 및 Azure 측 사전 조건을 평가합니다. 커넥터를 생성하지 않습니다.

**`get_connector_setup_instructions`** - 패키징되고 지원되는 Azure 온보딩 스크립트에서 정확한 발췌문을 반환합니다. 스크립트는 실행되지 않습니다.

# Security Hub의 사용량 및 비용 모니터링

사용량 페이지를 통해 조직 전체에서 Security Hub를 실행하는 데 드는 비용을 파악하고 관리할 수 있습니다. 이 페이지에서 현재 비용을 보고, 예상 월별 비용을 보고, 기능 또는 계정별 사용량을 탐색하고, 지출을 최적화하기 위한 전략을 찾을 수 있습니다.

## 사용 페이지에 액세스할 수 있는 사용자

사용 페이지는 Security Hub가 활성화된 모든 계정에서 사용할 수 있습니다. 액세스하려면 Security Hub 콘솔을 열고 탐색 창의 설정에서 사용을 선택합니다.

> **Important**
>
> 계정이 AWS Organization의 멤버 계정이고 Security Hub 위임된 관리자가 지정되지 않은 경우 사용 데이터를 사용할 수 없습니다. 사용 데이터를 보려면 조직의 관리 계정이 위임된 관리자를 지정해야 합니다. 자세한 내용은 the section called “위임 관리자 지정” 단원을 참조하십시오.

경험은 계정 유형에 따라 다릅니다.

- 위임된 관리자 또는 관리 계정 - 조직 비용 요약, 기능별 사용, 계정별 사용 및 비용 최적화 전략이 포함된 전체 사용 페이지가 표시됩니다.
- 멤버 계정 또는 독립 실행형 계정 - 계정의 기능별 사용량이 포함된 계정 비용 요약만 표시됩니다. 단일 계정을 보고 있으므로 계정별 탭을 사용할 수 없습니다.

## 조직 및 계정 비용 요약

> **Note**
>
> 조직 비용 요약 섹션은 위임된 관리자 계정 또는 관리 계정에서만 볼 수 있습니다. 멤버 계정과 독립 실행형 계정에는 대신 계정 비용 요약이 표시됩니다.

위임된 관리자 또는 관리 계정에서 사용 페이지를 열면 조직 비용 요약 섹션에 현재 결제 주기에 대한 조직의 Security Hub 비용에 대한 개략적인 개요가 표시됩니다. 이 섹션에는 다음이 포함되어 있습니다.

- 마지막으로 새로 고친 데이터 - Security Hub가 조직의 사용 데이터를 마지막으로 새로 고친 날짜입니다. Security Hub는이 데이터를 주기적으로 새로 고칩니다. 사용 페이지를 방문할 때 데이터가 24시간 이상 지난 경우 Security Hub는 자동으로 새로 고침을 트리거합니다. 조직의 크기에 따라 몇 시간 내에 새로 고침이 완료됩니다. 데이터를 새로 고치는 동안 데이터를 곧 사용할 수 있다는 메시지와 함께 알림이 나타납니다.
- 현재 비용 - 현재 결제 주기 시작부터 데이터가 마지막으로 새로 고쳐진 날짜까지 조직에서 Security Hub를 사용하는 데 발생한 총 금액입니다.
- 예상 월별 비용(30일) - 전체 30일 결제 주기로 추정된 지난 7일 사용량을 기준으로 한 예상 월별 비용입니다. 이 예측에는 유료 및 무료 평가판 사용량이 모두 포함되어 있어 월별 비용을 현실적으로 추정할 수 있습니다. 예상 비용은 협상한 할인(EDPs)을 고려하지 않습니다 AWS. 예상 비용이 현재 비용보다 낮은 것으로 보이는 경우, 즉 사용량이 감소하고 지난 7일 사용량을 기준으로 하면 30일 청구서가 현재 청구 주기의 청구서보다 낮아집니다.

## 기능 보기

기능 보기에는 보안 기능별로 조직된 전체 조직의 비용 및 사용량이 표시됩니다. 기능은 확장 가능한 세 그룹으로 구성됩니다. 각 그룹을 확장하거나 축소하여 그룹 내의 개별 사용 유형을 볼 수 있습니다. 각 사용 유형은 AWS Cost Explorer의 해당 사용 유형에 직접 매핑됩니다.

Security Hub 필수 계획 - EC2 인스턴스, ECR 컨테이너 이미지, Lambda 함수, IAM 사용자 및 IAM 역할을 모니터링합니다. 위험 및 노출 분석, 취약성 관리(Amazon Inspector 제공), 보안 태세 관리(Security Hub CSPM 제공) 및 보안 대응을 다룹니다. 이러한 모든 기능은 단일 리소스당 가격으로 필수 요금제에 포함되어 있으므로 Amazon Inspector 또는 AWS Security Hub CSPM을 별도로 활성화하거나 비용을 지불할 필요가 없으며 기본 서비스 사용에 대해 이중 요금이 부과되지 않습니다.

위협 분석 - CloudTrail 관리 이벤트 및 데이터 이벤트, 네트워크 활동 및 기타 로그를 포함합니다. 이러한 기능은 Amazon GuardDuty로 구동되는 위협 탐지를 다룹니다.

추가 기능 - Lambda 함수 코드 스캔을 포함합니다. 이는 보안 취약성에 대한 Lambda 함수 애플리케이션 코드를 분석하기 위해 Amazon Inspector에서 제공하는 선택적 개선 사항입니다.

각 기능의 요금에 대한 자세한 내용은 Security Hub 요금을 참조하세요.

이 보기의 표에는 각 사용 유형에 대한 다음 열이 포함되어 있습니다.

- 현재 사용량 - 결제 주기 시작부터 데이터가 마지막으로 새로 고쳐진 날짜까지 모든 계정 및 모든 리전에서이 사용 유형의 총 사용량입니다.

- 무료 사용 - 현재 무료 평가판에 있는 계정의이 사용 유형에 대한 총 사용 볼륨입니다. 사용 가능한 값은 녹색으로 표시됩니다.
- 현재 비용 - 결제 주기 시작부터 데이터가 마지막으로 새로 고쳐진 날짜까지 모든 계정 및 모든 리전에서이 사용 유형의 총 비용입니다.
- 무료 평가판 값 - 현재 무료 평가판에 있는 계정이 평가판에 없는 경우이 사용 유형에 대해 발생했을 비용입니다. 이렇게 하면 무료 평가판의 가치를 이해하는 데 도움이 됩니다.
- 예상 월별 비용(30일) - 모든 계정 및 모든 리전에서 지난 7일간의 사용량에서 추정된이 사용 유형의 예상 월별 비용입니다. 여기에는 예상 월별 비용을 제공하기 위한 유료 및 무료 평가판 사용이 모두 포함됩니다.

## 계정 보기

> **Note**
>
> 계정 보기는 위임된 관리자 계정 또는 관리 계정에서만 사용할 수 있습니다.

계정 보기를 선택하면 모든 리전의 개별 멤버 계정별로 구성된 비용을 볼 수 있습니다. 이 보기는 비용이 가장 많이 드는 계정을 식별하는 데 도움이 됩니다.

이 표에는 다음 열이 있는 각 계정이 나열되어 있습니다.

- 계정 - 클릭 가능한 링크로 표시되는 AWS 계정 ID입니다. 계정을 선택하면 세부 분석 패널이 열립니다.
- 현재 비용 - 모든 리전에서 결제 주기 시작부터 데이터가 마지막으로 새로 고쳐진 날짜까지이 계정의 총 비용입니다.
- 무료 평가판 값 -이 계정이 무료 평가판에 없는 경우 발생했을 비용입니다.
- 예상 월별 비용(30일) - 모든 리전에서 지난 7일 사용부터 전체 30일 결제 주기까지 추정된이 계정의 예상 월별 비용입니다. 예상에는 월별 비용에 대한 대표 견적을 제공하기 위한 유료 및 무료 평가판 사용량이 모두 포함됩니다. 예상 비용은 협상한 할인 AWS (EDPs)을 고려하지 않습니다.

  Security Hub가 지난 7일 이내에이 계정에서 활성화된 경우 예측은 활성화 이후 일수를 기준으로 합니다. 7일 후 프로젝션은 지난 7일 동안의 전체 사용량을 사용합니다. 사용 페이지는 현재 계정에서 Security Hub가 비활성화된 시기를 감지하지 못합니다. Security Hub가 최근에 하나 이상의 계정에서 비활성화된 경우 해당 계정은 사용량이 만료될 때까지 예측에 계속 표시됩니다. 이러한 변경 후 프로젝션이 조직의 업데이트된 상태를 반영할 때까지 7일이 걸립니다.

### 계정 세부 정보 보기

목록에서 계정을 선택하면 페이지 오른쪽에 세부 정보 패널이 열립니다. 이 패널에는 기능 보기와 동일한 기능 수준 분류가 표시되지만 해당 특정 계정으로 필터링됩니다. 모든 리전에서 해당 계정 내의 각 사용 유형에 대한 현재 사용량, 무료 사용량, 현재 비용, 무료 평가판 값 및 예상 월별 비용을 확인할 수 있습니다.

## 비용 최적화 전략

사용 페이지에서 비용 최적화 전략을 선택하여 보안 적용 범위를 유지하면서 비용을 관리하는 실행 가능한 방법이 포함된 전용 페이지로 이동합니다.

각 전략은 조직의 요구 사항에 따라 평가하고 적용할 수 있는 독립적인 옵션으로 제공됩니다. 보안 장단점이 없는 옵션이 먼저 나열됩니다. 전략을 적용한 후 변경 사항이 결제에 반영되려면 일반적으로 24~48시간이 걸립니다.

## 관련 리소스

- Security Hub 요금
- AWS Cost Explorer 사용 설명서

# Security Hub 비활성화

## 단일 계정에 대해 Security Hub 비활성화

계정이 조직의 일부가 아닌 경우 Security Hub 콘솔에서 언제든지 Security Hub를 비활성화하거나 DisableSecurityHubV2 API를 사용할 수 있습니다. Security Hub를 비활성화하면 탐지 엔진에서 조사 결과 수집이 중지되고 기존 조사 결과, 통합 및 구성에 대한 액세스 권한도 상실됩니다.

모든 리전에서 계정에 대해 Security Hub를 비활성화하면 Security Hub는 서비스를 활성화할 때 생성된 서비스 연결 IAM Access Analyzer도 삭제합니다. 자동 삭제에 실패하면 IAM Access Analyzer `DeleteServiceLinkedAnalyzer` API 작업을 호출하여 분석기를 삭제할 수 있습니다. 이 작업은 계정에 대해 Security Hub가 완전히 비활성화된 후에만 성공합니다. 단일 리전에서 Security Hub를 비활성화하지만 다른 리전에서는 활성화된 상태로 유지하면 미사용 액세스 분석기가 계속 실행되고 나머지 활성화된 리전에 결과가 계속 복제됩니다.

Security Hub 비활성화

1. 자격 증명으로 AWS 계정에 로그인하고 https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 일반을 선택합니다.
3. Security Hub에서 비활성화를 선택합니다. 팝업 창에서를 입력하고 비활성화를 **Disable**선택합니다.

# 조직 전체에서 Security Hub 비활성화

AWS 조직의 위임된 관리자인 경우 멤버 계정에서 Security Hub를 비활성화하는 두 가지 옵션이 있습니다.

## 옵션 1: 감지 엔진으로 Security Hub 비활성화

위임된 관리자 계정의 정책 카탈로그에서 Security Hub(필수 및 추가 기능) 배포 및 정책을 활용하여 특정 조직 단위, 계정 또는 리전에 대해 Amazon Inspector와 함께 Security Hub를 비활성화할 수 있습니다.

정책을 사용하여 멤버 계정에서 Security Hub 및 Amazon Inspector를 비활성화하려면

1. 위임된 관리자 자격 증명으로 AWS 계정을 사용하여 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 구성을 선택합니다.
3. 구성 카탈로그에서 Security Hub(필수 및 추가 기능)를 선택합니다.
4. 세부 정보 섹션의 Security Hub 구성 페이지에서 정책의 이름과 설명(예: "Security Hub 비활성화 정책")을 입력합니다.
5. 계정 선택 섹션에서 다음 옵션 중 하나를 선택합니다. 비활성화를 모든 조직 단위 및 계정에 적용하려면 모든 조직 단위 및 계정을 선택합니다. 특정 조직 단위 및 계정에 비활성화를 적용하려면 특정 조직 단위 및 계정을 선택합니다. 이 옵션을 선택하는 경우 검색 창 또는 조직 구조 트리를 사용하여 대상 조직 단위 및 계정을 지정합니다.
6. 리전 섹션에서 모든 리전 비활성화를 선택하여 모든 리전에서 Security Hub를 비활성화합니다. 선택적으로 새 리전을 자동으로 비활성화할지 여부를 선택합니다. 리전 지정을 선택하여 비활성화할 특정 리전을 선택합니다.
7. (선택 사항) 고급 설정은의 지침을 참조하세요 AWS Organizations.
8. (선택 사항) 리소스 태그의 경우 구성을 쉽게 식별할 수 있도록 태그를 키-값 페어로 추가합니다.

9. 다음을 선택합니다.
10. 변경 내용을 검토하고 적용을 선택합니다. 대상 계정이 정책에 따라 구성됩니다. 정책의 구성 상태가 정책 페이지 상단에 표시됩니다.

Amazon GuardDuty 및 AWS Security Hub CSPM 비활성화

GuardDuty 및 Security Hub CSPM 기능의 경우 각 위임된 관리자 계정에서 기능을 수동으로 비활성화해야 합니다. GuardDuty 및 Security Hub CSPM은 정책 대신 배포(일회성 작업)를 사용하므로 해당 콘솔에서 수동으로 비활성화를 수행해야 합니다.

## 옵션 2: Security Hub만 비활성화

기존 Security Hub 정책이 있고 Amazon Inspector, GuardDuty 또는 Security Hub CSPM에 영향을 주지 않고 Security Hub만 비활성화하려면 다음 단계를 따르세요.

멤버 계정 전체에서만 Security Hub를 비활성화하려면

1. 위임된 관리자 자격 증명으로 AWS 계정을 사용하여 로그인합니다. https://console.aws.amazon.com/securityhub/v2/home Security Hub 콘솔을 엽니다.
2. 탐색 창에서 관리를 선택한 다음 구성을 선택합니다.
3. 구성된 정책에서 Security Hub 정책을 선택합니다.
4. 정책 편집을 선택하고 계정 선택 섹션에서 다음 옵션 중 하나를 선택합니다. 비활성화를 모든 조직 단위 및 계정에 적용하려면 모든 조직 단위 및 계정을 선택합니다. 특정 조직 단위 및 계정에 비활성화를 적용하려면 특정 조직 단위 및 계정을 선택합니다. 이 옵션을 선택하는 경우 검색 창 또는 조직 구조 트리를 사용하여 대상 조직 단위 및 계정을 지정합니다.
5. 리전 섹션에서 모든 리전 비활성화를 선택하여 모든 리전에서 Security Hub를 비활성화합니다. 선택적으로 새 리전을 자동으로 비활성화할지 여부를 선택합니다. 리전 지정을 선택하여 비활성화할 특정 리전을 선택합니다.
6. (선택 사항) 고급 설정은 AWS Organizations의 지침을 참조하세요.
7. (선택 사항) 리소스 태그의 경우 구성을 쉽게 식별할 수 있도록 태그를 키-값 페어로 추가합니다.
8. 다음을 선택합니다.
9. 변경 내용을 검토하고 적용을 선택합니다. 대상 계정이 정책에 따라 구성됩니다. 정책의 구성 상태가 구성 페이지 상단에 표시됩니다.

다른 보안 서비스에 미치는 영향

Security Hub 정책을 통해 Security Hub를 비활성화해도 Security Hub CSPM, GuardDuty 및 Amazon Inspector 구성에는 영향을 주지 않습니다.

멤버 계정 간에만 Amazon Inspector를 비활성화해야 하는 경우 Security Hub 구성 카탈로그의 취약성 관리 정책을 사용할 수 있습니다. Security Hub 구성 페이지로 이동하여 Amazon Inspector에서 취약성 관리를 선택하고 위의 Security Hub 비활성화 절차와 유사한 단계에 따라 비활성화 정책을 생성합니다.

# AWSSecurity Hub의 보안

의 클라우드 보안AWS이 최우선 순위입니다. AWS고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS는 클라우드에서AWSAWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Security Hub에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 AWS 규정 준수 프로그램 제공 범위 내 서비스를 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Security Hub 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Security Hub를 구성하는 방법을 보여줍니다. 또한 Security Hub 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS서비스를 사용하는 방법을 알아봅니다.

주제

- AWSSecurity Hub의 데이터 보호
- AWS Security Hub의 Identity and Access Management
- AWS Security Hub에 대한 규정 준수 검증
- AWS Security Hub의 복원력
- AWS Security Hub의 인프라 보안

- AWS Security Hub 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

## AWSSecurity Hub의 데이터 보호

AWS 공동 책임 모델 AWSSecurity Hub의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ 참조하세요.  유럽의 데이터 보호에 대한 자세한 내용은 일반 데이터 보호 규정(GDPR) 센터를 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고AWS 계정 AWS IAM Identity Center또는 AWS Identity and Access Management(IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다AWS CloudTrail. CloudTrail 추적을 사용하여 AWS활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS암호화 솔루션을 사용합니다AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Security Hub 또는 기타AWS 서비스에서 콘솔AWS CLI, API 또는AWSSDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

Security Hub는 멀티 테넌트 서비스를 제공합니다. 데이터를 보호하기 위해 Security Hub는 저장된 데이터와 구성 요소 서비스 간에 전송 중인 데이터를 암호화합니다.

# 서비스 개선을 위한 데이터 사용 선택 해제

> **Note**
>
> 이 설명서 페이지는 2025년 12월 2일에 출시된 향상된 AWS Security Hub에만 적용됩니다. 원래 AWS Security Hub(현재 AWS Security Hub CSPM)의 고객인 경우 아래 설명된 데이터 사용량은 향상된 AWS Security Hub를 활성화한 후에만 적용됩니다.

AWS Organizations 옵트아웃 정책을 사용하여 AWS Security Hub 및 기타 AWS 보안 서비스를 개발하고 개선하는 데 데이터(Security Hub 서비스 약관에서 "Security Hub 콘텐츠"로 정의됨)를 사용하지 않도록 선택할 수 있습니다. Security Hub가 현재 이러한 콘텐츠를 수집하지 않더라도 옵트아웃하도록 선택할 수 있습니다. 옵트아웃 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AI 서비스 옵트아웃 정책을 참조하십시오.

> **Note**
>
> 옵트아웃 정책을 사용하려면 AWS Organizations에서 AWS 계정을 중앙에서 관리해야 합니다. AWS 계정에 대한 조직을 아직 생성하지 않은 경우 AWS Organizations 사용 설명서의 조직 생성 및 관리를 참조하세요.

옵트아웃은 다음과 같은 효과가 있습니다.

- Security Hub는 옵트아웃(있는 경우) 전에 서비스 개선을 위해 수집 및 저장된 콘텐츠를 삭제합니다.
- 옵트아웃하면 Security Hub는 더 이상 서비스 개선을 위해이 콘텐츠를 수집하거나 저장하지 않습니다.

다음 섹션에서는 Security Hub가 서비스 개선을 위해 콘텐츠를 처리하는 방법을 설명합니다.

AWS Security Hub 데이터 사용량

현재 AWS Security Hub는 서비스 개선을 위해 Security Hub 콘텐츠를 수집하거나 저장하지 않습니다. 그러나 향후 Security Hub는 Security Hub 및 기타 보안 서비스 기능을 개선하기 위해 Security Hub 및 기타 형태의 Security Hub 콘텐츠(Security Hub가 Security Hub 기능을 제공하기 위해 사용자 또는 업스트림 서비스로부터 수신하는 콘텐츠)에서 집계한 타사 AWS 보안 조사 결과를 수집하고 사용할 수 있습니다.

콘텐츠의 신뢰, 개인 정보 보호 및 보안이 가장 우선합니다. Security Hub가 향후 서비스 개선을 위해 Security Hub 콘텐츠 수집을 시작하는 경우이 페이지는 이러한 변경 사항을 반영하고 수집되는 데이터와 사용 방법에 대한 세부 정보를 제공하도록 업데이트됩니다. 위에서 설명한 AWS Organizations 옵트아웃 정책을 사용하여 언제든지이 Security Hub 콘텐츠 컬렉션을 옵트아웃할 수 있습니다. AWS 데이터 프라이버시 관행에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요.

참조

다른 AWS 보안 서비스의 유사한 옵트아웃 절차는 다음을 참조하세요.

- Amazon GuardDuty 사용 설명서의 서비스 개선을 위해 데이터 사용을 옵트아웃합니다.
- Amazon Security Lake 사용 설명서의 서비스 개선을 위해 데이터 사용을 옵트아웃합니다.

## AWS Security Hub의 Identity and Access Management

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 어떤 사용자가 Security Hub 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 소유)될 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- IAM에서 Security Hub의 작동 방식
- 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM
- AWS Security Hub의 서비스 연결 역할
- AWSSecurity Hub에 대한 관리형 정책
- AWS Security Hub 자격 증명 및 액세스 문제 해결

### 대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조AWS Security Hub 자격 증명 및 액세스 문제 해결)

- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(IAM에서 Security Hub의 작동 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 참조)

## ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리의 경우를 사용합니다 AWS IAM Identity Center. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 가장 좋습니다. 자세한 내용은 IAM 사용 설명서의 자

격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

## 정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

### 리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

### 기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

### 여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

## IAM에서 Security Hub의 작동 방식

AWS Identity and Access Management (IAM)를 사용하여 AWS Security Hub에 대한 액세스를 관리하기 전에 Security Hub에서 사용할 수 있는 IAM 기능을 알아봅니다.

AWS Security Hub에서 사용할 수 있는 IAM 기능

| IAM 기능 | Security Hub 지원 |
| --- | --- |
| 자격 증명 기반 정책 | 예 |

| IAM 기능 | Security Hub 지원 |
| --- | --- |
| 리소스 기반 정책 | 아니요 |
| 정책 작업 | 예 |
| 정책 리소스 | 아니요 |
| 정책 조건 키 | 예 |
| 액세스 제어 목록(ACL) | 아니요 |
| ABAC(속성 기반 액세스 제어) - 정책 태그 | 예 |
| 임시 보안 인증 | 예 |
| 전달 액세스 세션(FAS) | 예 |
| 서비스 역할 | 아니요 |
| 서비스 연결 역할 | 예 |

Security Hub 및 기타에서 대부분의 IAM 기능을 AWS 서비스 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS 서비스 IAM으로 작업하는 섹션을 참조하세요.

Security Hub에 대한 ID 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용자 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Security Hub는 ID 기반 정책을 지원합니다. 자세한 내용은 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 단원을 참조하십시오.

Security Hub의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 교차 계정 리소스 액세스를 참조하세요.

Security Hub는 리소스 기반 정책을 지원하지 않습니다. IAM 정책을 Security Hub 리소스에 직접 연결할 수 없습니다.

Security Hub의 정책 조치

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함합니다.

Security Hub의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
securityhub:
```

예를 들어, Security Hub API의 `EnableSecurityHubV2` 작업에 해당하는 작업인 Security Hub를 활성화할 수 있는 권한을 사용자에게 부여하려면 해당 `securityhub:EnableSecurityHubV2` 작업을 정책에 포함합니다. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Security Hub는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

```
"Action": "securityhub:EnableSecurityHubV2"
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다. 예제:

```
"Action": [
      "securityhub:EnableSecurityHubV2",
      "securityhub:CreateAutomationRuleV2"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수도 있습니다. 예를 들어, Get라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "securityhub:Get*"
```

하지만 가장 좋은 방법은 최소 권한의 원칙을 따르는 정책을 만드는 것입니다. 즉, 특정 작업을 수행하는 데 필요한 권한만 포함하는 정책을 만들어야 합니다.

Security Hub 작업 목록은 서비스 승인 참조의 AWS Security Hub에서 정의한 작업을 참조하세요. Security Hub 작업을 지정하는 정책의 예제는 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 섹션을 참조하세요.

Security Hub의 정책 리소스

정책 리소스 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Security Hub는 다음과 같은 리소스 유형을 정의합니다.

- Hub(허브)
- 제품
- 교차 리전 집계자라고도 하는 조사 결과 집계자
- 자동화 규칙

ARN을 사용하여 정책에서 이러한 유형의 리소스를 지정할 수 있습니다.

Security Hub 리소스 유형 및 각 리소스의 ARN 구문 목록은 서비스 승인 참조의 AWS Security Hub에서 정의한 리소스를 참조하세요. 각 리소스 유형에 대해 지정할 수 있는 작업을 알아보려면 서비스 승인 참조의 AWS Security Hub에서 정의한 작업을 참조하세요. 리소스를 지정하는 정책의 예제는 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 섹션을 참조하세요.

Security Hub에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Security Hub 조건 키 목록은 서비스 승인 참조의 AWS Security Hub에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 AWS Security Hub에서 정의한 작업을 참조하세요. 조건 키를 사용하는 정책의 예제는 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM을 참조하세요.

Security Hub의 액세스 제어 목록 (ACL)

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Security Hub는 ACLs 지원하지 않습니다. 즉, ACL을 Security Hub 리소스에 연결할 수 없습니다.

Security Hub의 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용자 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Security Hub 리소스에 태그를 연결할 수 있습니다. 또한 정책 `Condition` 요소에 태그 정보를 제공하여 리소스에 대한 액세스를 제어할 수도 있습니다.

Security Hub 리소스 태그를 지정하는 방법에 대한 자세한 내용은 Security Hub 리소스 태그 지정을 참조하세요. 태그를 기반으로 리소스에 대한 액세스를 제한하는 ID 기반 정책의 예제는 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 섹션을 참조하세요.

Security Hub에 대한 임시 보안 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용자 설명서의 IAM 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole 또는 GetFederationToken과 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

Security Hub에서 임시 자격 증명 사용을 지원합니다.

Security Hub에 대한 액세스 세션 전달

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

예를 들어 Security Hub는 Security Hub를와 AWS 서비스 통합 AWS Organizations 하고 Organizations에서 조직의 위임된 Security Hub 관리자 계정을 지정할 때 다운스트림에 FAS 요청을 보냅니다.

다른 작업의 경우, Security Hub는 사용자를 대신하여 작업을 수행하기 위해 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 AWS Security Hub의 서비스 연결 역할 섹션을 참조하세요.

### Security Hub의 서비스 역할

Security Hub는 서비스 역할을 수임하거나 사용하지 않습니다. Security Hub는 사용자를 대신하여 작업을 수행하기 위해 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 AWS Security Hub의 서비스 연결 역할 섹션을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Security Hub 사용 시 운영상 문제가 발생할 수 있습니다. Security Hub에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

### Security Hub의 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 태스크를 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Security Hub는 사용자를 대신하여 작업을 수행하기 위해 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 AWS Security Hub의 서비스 연결 역할 섹션을 참조하세요.

## 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM

기본적으로 사용자 및 역할은 Security Hub CSPM 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 관리자는 지정된 리소스에서 특정 API 태스크를 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용자 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Security Hub CSPM 콘솔 사용
- 예제: 사용자가 자신이 권한을 볼 수 있도록 허용
- 예제: 사용자가 조사 결과를 볼 수 있도록 허용

- 예제: 사용자가 자동화 규칙을 생성하고 관리하도록 허용

### 정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Security Hub 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

### Security Hub CSPM 콘솔 사용

AWS Security Hub CSPM 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 Security Hub CSPM 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정.

최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 생성하는 경우 콘솔은 해당 정책을 사용하는 엔터티(사용자 또는 역할)에 대해 의도한 대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

이러한 사용자 및 역할이 Security Hub CSPM 콘솔을 사용할 수 있도록 하려면 다음 AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용자 설명서의 사용자에게 권한 추가를 참조하세요.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

예제: 사용자가 자신이 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여 줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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": "*"
        }
    ]
}
```

예제: 사용자가 조사 결과를 볼 수 있도록 허용

이 예제에서는 사용자가 Security Hub CSPM 결과를 볼 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
```

```
                "securityhub:GetFindingsV2"
            ],
            "Resource": "*"
        }
    ]
}
```

예제: 사용자가 자동화 규칙을 생성하고 관리하도록 허용

이 예제에서는 사용자가 Security Hub CSPM 자동화 규칙을 생성, 보기, 업데이트 및 삭제할 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다. 이 IAM 정책이 작동하려면 사용자가 Security Hub CSPM 관리자여야 합니다. 예를 들어, 사용자가 자동화 규칙만 볼 수 있도록 권한을 허용하려면 생성, 업데이트 및 삭제 권한을 제거할 수 있습니다.

```
{
            "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": "*"
        }
```

```
    ]
}
```

## AWS Security Hub의 서비스 연결 역할

AWS Security Hub는 라는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다AWSServiceRoleForSecurityHubV2. 이 서비스 연결 역할은 Security Hub에 직접 연결된 IAM 역할입니다. Security Hub에서 사전 정의하며, Security Hub가 사용자를 대신하여 다른를 호출 AWS 서비스 하고 AWS 리소스를 모니터링하는 데 필요한 모든 권한을 포함합니다. Security Hub는 Security Hub를 사용할 수 AWS 리전 있는 모든에서이 서비스 연결 역할을 사용합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할을 사용하면 Security Hub를 더 쉽게 설정할 수 있습니다. Security Hub가 이 서비스 연결 역할 권한을 정의하므로, 달리 정의되지 않은 한 Security Hub만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 해당 권한 정책을 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할의 세부 정보를 검토하려면 Security Hub 콘솔을 사용할 수 있습니다. 탐색 창의 설정 아래에서 일반을 선택합니다. 그런 다음 서비스 권한 섹션에서 서비스 권한 보기를 선택합니다.

Security Hub가 활성화된 모든 리전에서 Security Hub를 비활성화한 후에만 Security Hub 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 액세스 권한을 실수로 제거할 수 없으므로 Security Hub 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM 사용자 설명서에서 IAM으로 작업하는AWS 서비스를 살펴보고 서비스 연결 역할 열이 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

주제

- Security Hub에 대한 서비스 연결 역할 권한
- Security Hub에 대한 서비스 연결 역할 생성
- Security Hub에 대한 서비스 연결 역할 편집
- Security Hub에 대한 서비스 연결 역할 삭제

### Security Hub에 대한 서비스 연결 역할 권한

Security Hub에서는 AWSServiceRoleForSecurityHubV2인 서비스 연결 역할을 사용합니다. 이는 AWS Security Hub가 리소스에 액세스하는 데 필요한 서비스 연결 역할입니다. 이 서

비스 연결 역할을 통해 Security Hub는 다른 로부터 조사 결과를 수신 AWS 서비스 하고 제어에 대한 보안 검사를 실행하는 데 필요한 AWS Config 인프라를 구성하는 등의 작업을 수행할 수 있습니다. AWSServiceRoleForSecurityHubV2 서비스 연결 역할은 역할을 수임하기 위해 securityhub.amazonaws.com서비스를 신뢰합니다.

AWSServiceRoleForSecurityHubV2 서비스 연결 역할은 관리형 정책 AWSSecurityHubV2ServiceRolePolicy을(를) 사용합니다.

IAM ID(역할, 그룹, 사용자 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 부여해야 합니다. AWSServiceRoleForSecurityHubV2 서비스 연결 역할을 성공적으로 생성하기 위해서는 Security Hub에 액세스 하기 위해 사용하는 IAM ID가 필수 권한이 있어야 합니다. 필수 권한을 부여하려면 다음 정책을 IAM ID에 연결하세요.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

Security Hub에 대한 서비스 연결 역할 생성

AWSServiceRoleForSecurityHubV2 서비스 연결 역할은 처음으로 Security Hub를 활성화하거나 이전에 Security Hub를 활성화하지 않은 리전에서 Security Hub를 활성화할 때 자동으로 생성됩니다.

또한 IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AWSServiceRoleForSecurityHubV2 서비스 연결 역할을 수동으로 생성할 수 있습니다. 수동 서비스 역할 생성에 대한 자세한 내용은 IAM 사용자 설명서의 서비스에 대한 역할 만들기를 참조하세요.

> **Important**
>
> Security Hub 관리자 계정에 대해 생성된 서비스 연결 역할은 연결된 Security Hub 멤버 계정에 적용되지 않습니다.

### Security Hub에 대한 서비스 연결 역할 편집

Security Hub에서는 AWSServiceRoleForSecurityHubV2 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 정보는 IAM 사용자 설명서의 서비스 연결 역할 편집을 참조하세요.

### Security Hub에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스를 더 이상 사용할 필요가 없는 경우 역할을 삭제합니다. 이렇게 하면 적극적으로 모니터링되거나 유지 관리되지 않는 미사용 엔터티가 없습니다.

Security Hub를 비활성화해도 Security Hub는 AWSServiceRoleForSecurityHubV2 서비스 연결 역할을 자동으로 삭제하지 않습니다. Security Hub를 다시 활성화하는 경우에는 기존 서비스 연결 역할을 다시 사용할 수 있습니다. Security Hub를 더 이상 사용할 필요가 없는 경우 서비스 연결 역할을 수동으로 삭제할 수 있습니다.

> **Important**
>
> AWSServiceRoleForSecurityHubV2 서비스 연결 역할을 삭제하기 전에 먼저 Security Hub가 활성화된 모든 리전에서 Security Hub를 비활성화해야 합니다. 자세한 내용은 Security Hub 비활성화 단원을 참조하십시오. 서비스 연결 역할을 삭제하려고 할 때 Security Hub가 비활성화되지 않으면 삭제가 실패합니다.

AWSServiceRoleForSecurityHubV2 서비스 연결 역할을 삭제하려면 IAM 콘솔, IAM CLI 또는 IAM API를 사용할 수 있습니다. 자세한 내용은 IAM 사용자 설명서에서 서비스 연결 역할 삭제를 참조하세요.

## AWSSecurity Hub에 대한 관리형 정책

AWS관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다AWS. AWS관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS관리형 정책은 모든 AWS고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS업데이트하는AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWSAWS 서비스는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

### AWS관리형 정책: AWSSecurityHubFullAccess

`AWSSecurityHubFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 모든 Security Hub 작업에 대한 전체 액세스 권한을 허용하는 관리 권한을 보안 주체에게 부여합니다. 보안 주체가 자신의 계정에 대해 Security Hub를 수동으로 활성화하려면 먼저 보안 주체에 이 정책을 연결해야 합니다. 예를 들어, 이러한 권한이 있는 보안 주체는 조사 결과의 상태를 보고 업데이트할 수 있습니다. 또한 사용자 지정 인사이트를 구성하고, 통합을 활성화하고, 표준 및 제어를 활성화/비활성화할 수 있습니다. 관리자 계정의 보안 주체는 멤버 계정을 관리할 수도 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `securityhub` – 보안 주체가 Security Hub 작업에 대한 모든 액세스 권한을 가질 수 있습니다.
- `guardduty` – 보안 주체가 Amazon GuardDuty의 계정 상태에 대한 정보를 가져올 수 있습니다.
- `iam` - 보안 주체가 Security Hub에 대한 서비스 연결 역할을 생성할 수 있도록 허용합니다.
- `inspector` – 보안 주체가 Amazon Inspector의 계정 상태에 대한 정보를 가져올 수 있습니다.
- `pricing` - 보안 주체가 AWS 서비스및 제품의 가격 목록을 가져올 수 있도록 허용합니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubFullAccess를 참조하세요.

### AWS관리형 정책: AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 Security Hub의 정보를 볼 수 있는 읽기 전용 권한을 사용자에게 부여합니다. 이 정책이 연결된 보안 주체는 Security Hub에서 업데이트를 수행할 수 없습니다. 예를 들어, 이러한 권한이 있는 보안 주체는 자신의 계정과 연결된 조사 결과 목록을 볼 수 있지만 조사 결과의 상태를 변경할 수는 없습니다. 이들은 인사이트 결과는 볼 수 있지만 사용자 지정 인사이트를 만들거나 구성할 수는 없습니다. 이들은 제어 기능 또는 제품 통합을 구성할 수 없습니다.

#### 권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `securityhub` - 사용자가 항목 목록 또는 특정 항목의 세부 정보를 반환하는 작업을 수행할 수 있습니다. 여기에는 `Get`, `List` 또는 `Describe`(으)로 시작하는 API 작업이 포함됩니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubReadOnlyAccess를 참조하세요.

### AWS관리형 정책: AWSSecurityHubOrganizationsAccess

`AWSSecurityHubOrganizationsAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 조직의 Security Hub를 활성화하고 관리할 수 있는 관리 권한을 부여합니다AWS Organizations. 이 정책에 대한 권한을 통해 조직 관리 계정은 Security Hub의 위임된 관리자 계정을 지정할 수 있습니다. 또한, 위임된 관리자 계정을 통해 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

이 정책은에 대한 권한만 제공합니다AWS Organizations. 조직 관리 계정 및 위임된 관리자 계정에도 관련 작업에 대한 권한이 필요합니다. `AWSSecurityHubFullAccess` 관리형 정책을 사용하여 이러한 권한을 부여할 수 있습니다.

#### 권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations:ListAccounts` – 보안 주체가 조직의 일부인 계정 목록을 검색할 수 있습니다.
- `organizations:DescribeOrganization` – 보안 주체가 조직에 대한 정보를 검색할 수 있습니다.
- `organizations:ListRoots` – 보안 주체가 조직의 루트를 나열할 수 있습니다.

- organizations:ListDelegatedAdministrators - 보안 주체가 조직의 위임된 관리자를 나열할 수 있습니다.
- organizations:ListAWSServiceAccessForOrganization - 보안 주체AWS 서비스가 조직에서 사용하는를 나열할 수 있도록 허용합니다.
- organizations:ListOrganizationalUnitsForParent – 보안 주체가 상위 OU의 하위 조직 단위(OU)를 나열할 수 있습니다.
- organizations:ListAccountsForParent – 보안 주체가 상위 OU의 하위 계정을 나열할 수 있습니다.
- organizations:ListParents - 지정된 하위 조직 단위(OU) 또는 계정의 직속 상위 역할을 하는 루트 또는 OU를 나열합니다.
- organizations:DescribeAccount – 보안 주체가 조직의 계정에 대한 정보를 검색할 수 있습니다.
- organizations:DescribeOrganizationalUnit – 보안 주체가 조직의 OU에 대한 정보를 검색할 수 있습니다.
- organizations:ListPolicies - 지정된 유형의 조직에 있는 모든 정책의 목록을 검색합니다.
- organizations:ListPoliciesForTarget - 지정된 대상 루트, 조직 단위(OU) 또는 계정에 직접 연결된 정책을 나열합니다.
- organizations:ListTargetsForPolicy - 지정된 정책이 연결된 모든 루트, 조직 단위(OU) 및 계정을 나열합니다.
- organizations:EnableAWSServiceAccess – 위탁자가 Organizations를 통합할 수 있도록 허용합니다.
- organizations:RegisterDelegatedAdministrator – 위탁자가 위임된 관리자 계정을 지정할 수 있도록 허용합니다.
- organizations:DeregisterDelegatedAdministrator – 위탁자가 위임된 관리자 계정을 제거할 수 있도록 허용합니다.
- organizations:DescribePolicy - 정책에 대한 정보를 검색합니다.
- organizations:DescribeEffectivePolicy - 지정된 정책 유형 및 계정에 대한 유효 정책의 내용을 반환합니다.
- organizations:CreatePolicy - 루트, 조직 단위(OU) 또는 개별 AWS계정에 연결할 수 있는 지정된 유형의 정책을 생성합니다.
- organizations:UpdatePolicy - 기존의 정책을 새로운 이름, 설명 또는 내용으로 업데이트합니다.
- organizations:DeletePolicy - 조직에서 지정된 정책을 삭제합니다.

- `organizations:AttachPolicy` - 정책을 루트, 조직 단위(OU) 또는 개인 계정에 연결합니다.
- `organizations:DetachPolicy` - 대상 루트, 조직 단위(OU) 또는 계정에서 정책을 분리합니다.
- `organizations:EnablePolicyType` - 루트에서 정책 유형을 활성화합니다.
- `organizations:DisablePolicyType` - 루트에서 조직 정책 유형을 비활성화합니다.
- `organizations:TagResource` - 지정된 리소스에 하나 이상의 태그를 추가합니다.
- `organizations:UntagResource` - 지정된 리소스에서 지정된 키가 있는 태그를 모두 제거합니다.
- `organizations:ListTagsForResource` - 지정된 리소스에 연결된 태그를 나열합니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubOrganizationsAccess를 참조하세요.

AWS관리형 정책: AWSSecurityHubV2ServiceRolePolicy

이 정책을 통해 Security Hub는 조직 및 사용자를 대신하여 AWS Config규칙 및 Security Hub 리소스를 관리할 수 있습니다. 이 정책은 서비스에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 이 정책을 IAM 자격 증명에 연결할 수 없습니다. 자세한 내용은 the section called “서비스 연결 역할” 단원을 참조하십시오.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `access-analyzer` - 고객이 Security Hub를 활성화 또는 비활성화할 때 서비스 연결 IAM Access Analyzer를 생성 및 삭제하고, 분석기를 나열하여 분석기 상태가 활성화 상태와 일치하는지 확인하고, 미사용 액세스 결과에 대한 정책 권장 사항을 생성 및 검색합니다.
- `cloudwatch` - Security Hub 리소스 및 커넥터 상태 지표에 대한 측정 기능을 지원하는 지표 데이터를 검색합니다.
- `config` - 글로벌 Config 레코더에 대한 지원을 포함하여 Security Hub 리소스에 대한 서비스 연결 구성 레코더 및 타사 서비스 연결 구성 레코더를 관리합니다. 구성 레코더를 나열하고 타사 클라우드 통합을 지원하는 커넥터 정보를 가져옵니다.
- `ecr` - Amazon Elastic Container Registry 이미지 및 리포지토리에 대한 정보를 검색하여 측정 기능을 지원합니다.
- `iam` - 서비스 연결 역할, 즉 고객 계정의 AWS ConfigIAM Access Analyzer 및 타사 스캔을 위한 Amazon Inspector를 생성합니다. 계정 정보를 검색하여 측정 기능을 지원합니다. 고객이 현재 정책과 권장되는 최소 권한 대체의 비교를 볼 수 있도록 기존 IAM 정책을 검색합니다.

- `inspector2` - 타사 클라우드 통합을 지원하기 위해 Amazon Inspector 커넥터 및 커넥터 스캔 구성을 생성, 업데이트, 삭제 및 나열합니다.
- `lambda` - 측정 기능을 지원하는 AWS Lambda함수 정보를 검색합니다.
- `organizations` – 조직의 계정 및 OU(조직 단위) 정보를 검색합니다.
- `securityhub` - Security Hub 구성을 관리합니다. 타사 클라우드 통합을 지원하기 위해 Security Hub 커넥터를 생성, 업데이트 및 삭제합니다.
- `sts` - 서드 파티 클라우드 통합을 지원하기 위해 아웃바운드 자격 증명 연동을 위한 웹 자격 증명 토큰을 얻습니다.
- `tag` – 리소스 태그에 대한 정보를 검색합니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubV2ServiceRolePolicy를 참조하세요.

AWS관리형 정책에 대한 Security Hub 업데이트

다음 표에는이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 AWSSecurity Hub의 AWS관리형 정책 업데이트에 대한 세부 정보가 나와 있습니다. 이 정책의 업데이트에 대한 자동 알림을 받으려면 Security Hub 문서 기록 페이지에서 RSS 피드를 구독하세요.

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubV2ServiceRolePolicy – 업데이트된 정책 | Security Hub는 타사 통합을 지원하도록 정책을 업데이트했습니다. 이 업데이트에는 타사 구성 레코더 관리, Security Hub 및 Amazon Inspector 커넥터 생성 및 관리, CloudWatch에서 커넥터 상태 지표 검색, 타사 스캔을 위한 Amazon Inspector 서비스 연결 역할 생성, 페더레이션을 위한 웹 자격 증명 토큰 획득 권한이 추가되었습니다. | 2026년 6월 30일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubV2ServiceRolePolicy – 업데이트된 정책 | Security Hub는 IAM Access Analyzer 권한을 추가하도록 정책을 업데이트했습니다. 업데이트를 통해 Security Hub는 서비스 관리형 분석기를 생성 및 관리하고, 분석기를 나열하여 분석기 구성이 활성화 상태와 일치하는지 확인하고, 미사용 액세스 결과에 대한 정책 권장 사항을 생성 및 검색하고, 권장 사항 표시를 위한 IAM 정책을 검색할 수 있습니다. | 2026년 5월 10일 |
| AWSSecurityHubOrganizationsAccess – 업데이트된 정책 | Security Hub는 Security Hub 기능을 지원하는 리소스 정책을 설명하는 권한을 추가하도록 정책을 업데이트했습니다. Security Hub는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. | 2025년 11월 12일 |
| AWSSecurityHubFullAccess – 업데이트된 정책 | Security Hub는 Security Hub 기능을 지원하기 위해 GuardDuty, Amazon Inspector 및 계정 관리 관리에 대한 기능을 추가하도록 정책을 업데이트했습니다. Security Hub는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. | 2025년 11월 17일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubV2ServiceRolePolicy – 업데이트된 정책 | Security Hub는 Amazon Elastic Container Registry, AWS LambdaAmazon CloudWatch에 대한 측정 기능을 추가하고 Security Hub 기능을 지원AWS Identity and Access Management하도록 정책을 업데이트했습니다. 이 업데이트에는 글로벌 AWS Config레코더에 대한 지원도 추가되었습니다. Security Hub는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. | 2025년 11월 5일 |
| AWSSecurityHubOrganizationsAccess – 기존 정책 업데이트 | Security Hub는 정책에 대한 새로운 권한을 추가했습니다. 이러한 권한을 통해 조직 관리는 조직의 Security Hub 및 Security Hub CSPM을 활성화하고 관리할 수 있습니다. | 2025년 6월 17일 |
| AWSSecurityHubFullAccess – 기존 정책 업데이트 | Security Hub CSPM은 위탁자가 Security Hub에 대한 서비스 연결 역할을 생성할 수 있는 새 권한을 추가했습니다. | 2025년 6월 17일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubV2ServiceRolePolicy – 새 정책 | Security Hub는 Security Hub가 고객 조직 및 고객을 대신하여 AWS Config규칙 및 Security Hub 리소스를 관리할 수 있도록 허용하는 새 정책을 추가했습니다. Security Hub는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. | 2025년 6월 17일 |
| AWSSecurityHubFullAccess – 기존 정책 업데이트 | Security Hub CSPM은 AWS 서비스및 제품에 대한 요금 세부 정보를 가져오도록 정책을 업데이트했습니다. | 2024년 4월 24일 |
| AWSSecurityHubReadOnlyAccess – 기존 정책 업데이트 | Security Hub CSPM은 `Sid` 필드를 추가하여 이 관리형 정책을 업데이트했습니다. | 2024년 2월 22일 |
| AWSSecurityHubFullAccess – 기존 정책 업데이트 | Security Hub CSPM은 Amazon GuardDuty 및 Amazon Inspector가 계정에서 활성화되어 있는지 확인할 수 있도록 정책을 업데이트했습니다. 이를 통해 고객은 여러의 보안 관련 정보를 통합할 수 있습니다AWS 서비스. | 2023년 11월 16일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubOrganizationsAccess – 기존 정책 업데이트 | Security Hub CSPM은 AWS Organizations 위임된 관리자 기능에 대한 읽기 전용 액세스를 허용하는 추가 권한을 부여하도록 정책을 업데이트했습니다. 여기에는 루트, 조직 단위(OU), 계정, 조직 구조 및 서비스 액세스와 같은 세부 정보가 포함됩니다. | 2023년 11월 16일 |
| AWSSecurityHubOrganizationsAccess – 새로운 정책 | Security Hub CSPM은 Security Hub CSPM과 Organizations의 통합에 필요한 권한을 부여하는 새로운 정책을 추가했습니다. | 2021년 3월 15일 |
| Security Hub CSPM이 변경 내용 추적을 시작했습니다 | Security Hub CSPM이 AWS관리형 정책에 대한 변경 사항 추적을 시작했습니다. | 2021년 3월 15일 |

## AWS Security Hub 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 AWS Security Hub 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- 본인은 Security Hub에서 작업을 수행할 권한이 없습니다.
- iam:PassRole을 수행하도록 인증되지 않음
- Security Hub에 프로그래밍 방식으로 액세스하고 싶습니다
- 관리자인데, 다른 사용자가 Security Hub에 액세스할 수 있게 허용하려고 함
- 내 외부의 사람이 내 Security Hub 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

본인은 Security Hub에서 작업을 수행할 권한이 없습니다.

에서 작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 사용자 `mateojackson`이 콘솔을 사용하여 *##*에 대한 세부 정보를 보려고 하지만 `securityhub:`*`GetWidget`* 권한이 없는 경우에 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

이 경우, Mateo는 *`my-example-widget`* 작업을 사용하여 `securityhub:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Security Hub에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Security Hub에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

Security Hub에 프로그래밍 방식으로 액세스하고 싶습니다

사용자는 AWS 외부에서와 상호 작용하려는 경우 프로그래밍 방식으로 액세스해야 합니다 AWS Management Console. 프로그래밍 방식 액세스를 부여하는 방법은에 액세스하는 사용자 유형에 따라 다릅니다 AWS.

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

| 프로그래밍 방식 액세스가 필요한 사용자 | 목적 | 방법 |
| --- | --- | --- |
| IAM | (권장) 콘솔 자격 증명을 임시 자격 증명으로 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다.<br>• 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 AWS 로컬 개발을 위한 로그인을 참조하세요.<br>• AWS SDKs 경우 SDK 및 도구 참조 안내서의 AWS 로컬 개발을 위한 로그인을 참조하세요. AWS SDKs |
| 작업 인력 ID<br><br>(IAM Identity Center에서 관리되는 사용자) | 임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다.<br>• 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 AWS CLI 를 사용하도록 구성을 AWS IAM Identity Center 참조하세요.<br>• AWS SDKs, 도구 및 AWS APIs 경우 SDK 및 도구 참조 안내서의 IAM Identity Center 인증을 참조하세요. AWS SDKs |
| IAM | 임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | IAM 사용 설명서의 AWS 리소스에서 임시 자격 증명 사용의 지침을 따릅니다. |
| IAM | (권장되지 않음) | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다. |

| 프로그래밍 방식 액세스가 필요한 사용자 | 목적 | 방법 |
| --- | --- | --- |
| | 장기 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | • 자세한 AWS CLI내용은 사용 AWS Command Line Interface 설명서의 IAM 사용자 자격 증명을 사용하여 인증을 참조하세요.<br>• AWS SDKs 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용하여 인증을 참조하세요. AWS SDKs<br>• AWS APIs 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요. |

관리자인데, 다른 사용자가 Security Hub에 액세스할 수 있게 허용하려고 함

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요.

- 의 사용자 및 그룹 AWS IAM Identity Center:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용자 안내서에서 권한 세트 생성의 지침을 따릅니다.
- ID 제공업체를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용자 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용자 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음) 정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따릅니다.

내 외부의 사람이 내 Security Hub 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Security Hub에서 이러한 기능을 지원하는지 여부를 알아보려면 IAM에서 Security Hub의 작동 방식 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

## AWS Security Hub에 대한 규정 준수 검증

새로운 AWS 가입 환경은 규제 워크로드용으로 설계되지 않았습니다. 새로운 AWS 가입 환경을 사용하고 있지만 규제 대상 워크로드 AWS 에를 사용하려는 경우 AWS 환경에 가입 AWS (고급)하거나 고급 기능을 활성화할 수 있습니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 제공 범위 내를 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 AWS 보안 설명서를 AWS 서비스참조하세요.

# AWS Security Hub의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며, 이러한 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

# AWS Security Hub의 인프라 보안

관리형 서비스인 AWS Security Hub는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요 AWS .

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Security Hub에 액세스합니다. 클라이언트는 다음을 지원해야 합니다.

- Transport Layer Security(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

# AWS Security Hub 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성하여 VPC와 AWS Security Hub 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 비공개로 Security Hub API에 액세스할 수 있도록 지원하는 AWS PrivateLink 기술로 구동됩니다. VPC의 인스턴스는 Security Hub APIs와 통신하는 데 퍼블릭 IP 주소가 필요하지 않습니다. VPC와 Security Hub 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 Elastic Network Interfaces로 표현됩니다. 자세한 내용은 Amazon Virtual Private Cloud 가이드의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

## Security Hub VPC 엔드포인트에 대한 고려 사항

Security Hub용 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon Virtual Private Cloud 설명서의 사전 조건 및 기타 정보를 검토해야 합니다.

Security Hub는 VPC에서 모든 API 작업에 대한 호출 수행을 지원합니다.

## Security Hub에 대한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 Security Hub 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 Amazon Virtual Private Cloud 설명서의 VPC 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 Security Hub용 VPC 종단점을 생성합니다.

`com.amazonaws.region.securityhub`

여기서 *region*은 해당 AWS 리전의 리전 코드입니다.

엔드포인트에 프라이빗 DNS를 사용하도록 설정하는 경우, 리전에 대한 기본 DNS 이름(예: `securityhub.us-east-1.amazonaws.com` 미국 동부(버지니아 북부) 리전)을 사용하여 Security Hub에 API 요청을 할 수 있습니다.

## Secrets Manager에 대한 VPC 엔드포인트 정책 생성

Security Hub에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스

자세한 내용은 Amazon Virtual Private Cloud 설명서의 엔드포인트 정책을 사용한 VPC 엔드포인트에 대한 액세스 제어를 참조하세요.

예제: Security Hub 작업에 대한 VPC 엔드포인트 정책

다음은 Security Hub에 대한 엔드포인트 정책의 예입니다. 이 정책은 엔드포인트에 연결될 때 모든 리소스의 모든 보안 주체에 대한 액세스 권한을 나열된 Security Hub 작업에 부여합니다.

```
{
```

```
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

### 공유 서브넷

공유하는 서브넷의 VPC 엔드포인트는 생성, 설명, 수정 또는 삭제할 수 없습니다. 그러나 공유하는 서브넷의 VPC 엔드포인트를 사용할 수는 있습니다. VPC 공유에 대한 자세한 내용은 Amazon Virtual Private Cloud 설명서의 다른 계정과 VPC 서브넷 공유를 참조하세요.

## CloudTrail을 사용하여 Security Hub API 직접 호출 로깅

는 Security Hub의 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Security Hub에 대한 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 직접 호출에는 Security Hub 콘솔에서 수행한 직접 호출과 Security Hub API 작업에 대한 코드 직접 호출이 포함됩니다. 추적을 생성하면 Security Hub 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail이 수집한 정보를 사용하여 Security Hub에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 사용 방법을 포함하여 CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

### CloudTrail의 Security Hub 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. Security Hub에서 지원되는 이벤트 활동이 발생하면 해당 활동은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Security Hub에 대한 이벤트를 포함하여 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 추가적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

Security Hub는 모든 Security Hub API 작업을 CloudTrail 로그에 이벤트로 로깅하는 것을 지원합니다. Security Hub 작업 목록을 보려면 Security Hub API 참조를 참조하세요.

다음 작업에 대한 작업이 CloudTrail에 로깅될 때 `responseElements`의 값은 `null`로 설정됩니다. 이렇게 하면 민감한 정보가 CloudTrail 로그에 포함되지 않습니다.

- `GetFindingsV2`

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

## 예제: Security Hub의 로그 파일 항목

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함하고 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출에 대한 순서 지정된 스택 추적이 아니기 때문에 특정 순서로 표시되지 않습니다.

다음은 CreateAutomationRuleV2 작업을 보여 주는 CloudTrail 로그 항목이 나타낸 예제입니다. 이 예제에서는 라는 자동화 규칙TestAutomationRule이 생성됩니다. Severity 및 Account ID 속성은 기준으로 지정됩니다. 규칙이 일치하면 Severity이 높음으로 업데이트됩니다. 자동화 규칙에 대한 자세한 내용은 섹션을 참조하세요Security Hub의 자동화 규칙.


```
{
    "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"
}
```

# AWS Security Hub CSPM 소개

AWS Security Hub Cloud Security Posture Management(AWS Security Hub CSPM)는의 보안 상태에 대한 포괄적인 보기를 AWS 제공하고 보안 업계 표준 및 모범 사례를 기준으로 AWS 환경을 평가하는 데 도움이 됩니다.

AWS Security Hub CSPM은 AWS 계정 AWS 서비스및 지원되는 타사 제품 전반에 걸쳐 보안 데이터를 수집하고 보안 추세를 분석하고 우선 순위가 가장 높은 보안 문제를 식별하는 데 도움이 됩니다.

조직의 보안 상태를 관리하는 데 도움이 되도록 Security Hub CSPM은 여러 보안 표준을 지원합니다. 여기에는에서 개발한 AWS 기본 보안 모범 사례(FSBP) 표준 AWS과 인터넷 보안 센터(CIS), 결제 카드 산업 데이터 보안 표준(PCI DSS), 미국 국립 표준 기술 연구소(NIST)와 같은 외부 규정 준수 프레임워크가 포함됩니다. 각 표준에는 몇 가지 보안 제어 기능이 포함되며, 각각의 보안 제어 기능은 보안 모범 사례를 나타냅니다. Security Hub CSPM은 보안 제어 기능에 대한 검사를 실행하고 제어 기능에 대한 조사 결과를 생성하여 보안 모범 사례에 대한 규정 준수를 평가하는 데 도움을 드립니다.

Security Hub CSPM은 제어 조사 결과를 생성하는 것 외에도 Amazon GuardDuty, Amazon Inspector 및 Amazon Macie와 AWS 서비스같은 다른의 조사 결과와 지원되는 타사 제품도 수신합니다. 이를 통해 사용자는 다양한 보안 관련 문제를 한 눈에 파악할 수 있습니다. Security Hub CSPM의 조사 결과를 다른 AWS 서비스 및 지원되는 서드 파티 제품에 보낼 수도 있습니다.

Security Hub CSPM은 보안 문제를 분류하고 해결하는 데 도움이 되는 자동화 기능을 제공합니다. 예를 들어, 보안 검사에 실패할 경우, 자동화 규칙을 사용하여 중요한 조사 결과를 자동으로 업데이트할 수 있습니다. 또한, Amazon EventBridge와의 통합을 활용하여 특정 조사 결과에 대해 자동 응답을 트리거할 수 있습니다.

주제


- Security Hub CSPM의 이점
- Security Hub CSPM 액세스
- 관련 서비스
- Security Hub CSPM 무료 평가판 및 요금
- Security Hub CSPM 개념 및 용어
- Security Hub CSPM 활성화
- Security Hub CSPM의 관리자 및 멤버 계정 관리
- Security Hub CSPM의 교차 리전 집계 이해
- Security Hub CSPM의 보안 표준 이해

- Security Hub CSPM의 보안 제어 이해
- Security Hub CSPM의 통합 이해
- Security Hub CSPM과 Microsoft Azure 통합
- Security Hub CSPM에서 조사 결과 생성 및 업데이트
- Security Hub CSPM에서 인사이트 보기
- Security Hub CSPM 조사 결과 자동 수정 및 조치
- Security Hub CSPM의 대시보드 작업
- Security Hub CSPM 리전 제한
- CloudFormation을 사용하여 Security Hub CSPM 리소스 생성
- Amazon SNS로 Security Hub CSPM 공지 구독
- Security Hub CSPM 비활성화
- 의 보안 AWS Security Hub CSPM
- CloudTrail을 사용하여 Security Hub API 직접 호출 로깅


# Security Hub CSPM의 이점

다음은 Security Hub CSPM이 AWS 환경 전반의 규정 준수 및 보안 태세를 모니터링하는 데 도움이 되는 몇 가지 주요 방법입니다.

조사 결과 수집 및 우선 순위 지정에 대한 노력 감소

Security Hub CSPM은 통합 및 AWS 서비스 AWS 파트너 제품의 계정 전체에서 보안 조사 결과를 수집하고 우선순위를 지정하는 노력을 줄입니다. Security Hub CSPM은 표준 결과 형식인 AWS Security Finding Format(ASFF)을 사용하여 결과 데이터를 처리합니다. 이렇게 하면 무수히 많은 소스에서 나온 조사 결과를 여러 형식으로 관리할 필요가 없습니다. Security Hub CSPM은 또한 가장 중요한 조사 결과에 우선순위를 지정할 수 있도록 공급자 간 조사 결과를 상호 연관시킵니다.

모범 사례 및 표준에 대한 자동 보안 검사

Security Hub CSPM은 AWS 모범 사례 및 업계 표준에 따라 지속적인 계정 수준 구성 및 보안 검사를 자동으로 실행합니다. Security Hub CSPM은 이러한 검사 결과를 사용하여 보안 점수를 계산하고 주의가 필요한 특정 계정과 리소스를 파악합니다.

여러 계정 및 공급자의 조사 결과 통합 보기

Security Hub CSPM은 계정 및 공급자 제품 전반에 걸친 보안 탐지 조사 결과를 통합하여 Security Hub CSPM 콘솔에 조사 결과를 표시합니다. Security Hub CSPM API AWS CLI또는 SDKs. 전반적

인 현재 보안 상태를 확인하여 추세를 파악하고 잠재적인 문제를 식별하며 필요한 수정 단계를 수행할 수 있습니다.

조사 결과 업데이트 및 수정 작업을 자동화하는 기능

정의된 기준에 따라 조사 결과를 수정하거나 숨기는 자동화 규칙을 만들 수 있습니다. 또한, Security Hub CSPM은 Amazon EventBridge와의 통합도 지원합니다. 특정 조사 결과의 수정 작업을 자동화하기 위해 조사 결과가 생성될 때 수행할 사용자 지정 작업을 정의할 수 있습니다. 예를 들어, 조사 결과를 티켓팅 시스템 또는 자동 문제 해결 시스템으로 전송하도록 사용자 지정 작업을 구성할 수 있습니다.

# Security Hub CSPM 액세스

Security Hub CSPM은 대부분에서 사용할 수 있습니다 AWS 리전. 현재 Security Hub CSPM을 사용할 수 있는 리전의 목록은 AWS 일반 참조의 AWS Security Hub CSPM 엔드포인트 및 할당량을 참조하세요. 에 대한 관리에 AWS 리전 대한 자세한 AWS 계정내용은 AWS Account Management 참조 안내서의 계정에서 사용할 수 있는 지정을 참조 AWS 리전하세요.

각 리전에서는 다음 방법 중 하나를 사용하여 Security Hub CSPM에 액세스하여 사용할 수 있습니다.

Security Hub CSPM 콘솔

는 리소스를 생성하고 관리하는 AWS 데 사용할 수 있는 브라우저 기반 인터페이스 AWS Management Console 입니다. 이 콘솔의 일부인 Security Hub CSPM 콘솔은 Security Hub CSPM 계정, 데이터 및 리소스에 대한 액세스를 제공합니다. Security Hub CSPM 콘솔을 사용하여 조사 결과 보기, 자동화 규칙 생성, 집계 영역 생성 등의 Security Hub CSPM 태스크를 수행할 수 있습니다.

Security Hub CSPM API

Security Hub CSPM API를 사용하면 프로그래밍 방식으로 Security Hub CSPM 계정, 데이터 및 리소스에 액세스할 수 있습니다. API를 사용하면 HTTPS 요청을 Security Hub CSPM에 직접 보낼 수 있습니다. API에 대한 자세한 내용은 AWS Security Hub API 참조 섹션을 참조하세요.

AWS CLI

를 사용하면 시스템의 명령줄에서 명령을 실행하여 Security Hub CSPM 작업을 수행할 AWS CLI수 있습니다. 경우에 따라 명령줄을 사용하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. 작업을 수행하는 스크립트를 작성할 때도 명령줄이 유용합니다. 설치 및 사용에 대한 자세한 내용은 AWS Command Line Interface 사용 설명서를 AWS CLI참조하세요.

AWS SDKs

AWS 는 Java, Go, Python, C++ 및 .NET과 같은 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리 및 샘플 코드로 구성된 SDKs를 제공합니다. SDKs를 사용하면 Security Hub CSPM 및 기타 AWS 서비스 에 원하는 언어로 프로그래밍 방식으로 편리하게 액세스할 수 있습니다. SDK는 요청에 암호화 방식으로 서명, 오류 관리 및 자동으로 요청 재시도와 같은 작업을 포함합니다. AWS SDKs. AWS

**Important**

Security Hub CSPM은 사용자가 Security Hub CSPM을 활성화한 후에 생성된 조사 결과만 감지하고 통합합니다. Security Hub CSPM를 활성화하기 전에 생성된 보안 조사 결과를 소급하여 탐지하고 통합하지 않습니다.
Security Hub CSPM은 계정에서 Security Hub CSPM을 활성화한 리전의 조사 결과만 수신하고 처리합니다.
CIS AWS 파운데이션 벤치마크 보안 검사를 완전히 준수하려면 지원되는 모든 AWS 리전에서 Security Hub CSPM을 활성화해야 합니다.

# 관련 서비스

AWS 환경을 더욱 안전하게 보호하려면 Security Hub CSPM과 함께 다른 AWS 서비스 를 사용하는 것이 좋습니다. 일부는 결과를 Security Hub CSPM으로 AWS 서비스 전송하고 Security Hub CSPM은 결과를 표준 형식으로 정규화합니다. Security Hub CSPM에서 조사 결과를 받을 수도 AWS 서비스 있습니다.

Security Hub CSPM 조사 결과를 보내거나 받는 기타 목록은 섹션을 참조 AWS 서비스 하세요AWS 서비스 Security Hub CSPM과의 통합.

Security Hub CSPM은의 서비스 연결 규칙을 사용하여 대부분의 제어 AWS Config 에 대한 보안 검사를 실행합니다. 제어는 특정 AWS 서비스 및 AWS 리소스를 참조합니다. Security Hub CSPM 제어 목록은 Security Hub CSPM 제어 참조 섹션을 참조하세요. Security Hub CSPM에서 대부분의 제어 조사 결과를 생성하려면 AWS Config 에서 리소스를 활성화 AWS Config 하고 기록해야 합니다. 자세한 내용은 활성화 및 구성 전 고려 사항 AWS Config 단원을 참조하십시오.

# Security Hub CSPM 무료 평가판 및 요금

에서 Security Hub CSPM AWS 계정 을 처음 활성화하면 해당 계정이 30일 Security Hub CSPM 무료 평가판에 자동으로 등록됩니다.

무료 평가판 중에 Security Hub CSPM을 사용하는 경우 AWS Config 항목과 같이 Security Hub CSPM이 상호 작용하는 다른 서비스의 사용에 대해 요금이 부과됩니다. Security Hub CSPM 보안 표준에 의해서만 활성화되는 AWS Config 규칙에 대해서는 요금이 부과되지 않습니다.

무료 평가판 기간이 종료할 때까지는 Security Hub CSPM 사용 요금이 청구되지 않습니다.

## 사용 세부 정보 보기

Security Hub CSPM은 계정에서 처리한 보안 검사 및 조사 결과 수를 포함한 사용 정보를 제공합니다. 사용 세부 정보에는 무료 평가판에 남은 시간도 포함됩니다. 이 정보는 무료 평가판이 종료된 후 Security Hub CSPM 사용량을 이해하는 데 도움이 될 수 있습니다. 무료 평가판 사용이 종료된 후에도 사용량 정보를 확인할 수 있습니다.

사용량 정보를 표시하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 사용량을 선택합니다.

사용 정보는 현재 계정 및 현재 리전에만 해당됩니다. 집계 리전에서 사용 정보에는 연결된 리전이 포함되지 않습니다. 연결된 리전에 대한 자세한 내용은 the section called “집계되는 데이터 유형” 섹션을 참조하세요.

계정의 비용 세부 정보를 보려면 AWS 결제 콘솔을 사용합니다.

## 요금 내역

Security Hub CSPM의 수집된 조사 결과 및 보안 검사에 대한 요금 부과 방법에 대한 자세한 내용은 Security Hub CSPM 요금을 참조하세요.

# Security Hub CSPM 개념 및 용어

AWS Security Hub CSPM에서는 일반적인 AWS 개념과 용어를 기반으로 이러한 추가 용어를 사용합니다.

Account

AWS 리소스가 포함된 표준 Amazon Web Services(AWS) 계정입니다. 계정으로에 로그인하고 Security Hub CSPM AWS 을 활성화할 수 있습니다.

계정은 다른 계정을 초대하여 Security Hub CSPM을 활성화하고 Security Hub CSPM에서 해당 계정에 연결할 수 있습니다. 멤버십 초대 수락은 선택 사항입니다. 초대가 수락되면 계정은 관리자 계정이 되며, 추가된 계정은 멤버 계정이 됩니다. 관리자 계정은 멤버 계정에 있는 조사 결과를 볼 수 있습니다.

에 등록하면 AWS Organizations조직에서 조직의 Security Hub CSPM 관리자 계정을 지정합니다. Security Hub CSPM 관리자 계정은 다른 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

한 계정이 관리자 계정이면서 동시에 멤버 계정일 수 없습니다. 계정에는 관리자 계정이 하나만 있을 수 있습니다.

자세한 내용은 Security Hub CSPM의 관리자 및 멤버 계정 관리 섹션을 참조하세요.

관리자 계정

연결된 멤버 계정의 조사 결과를 볼 수 있는 액세스 권한이 부여된 Security Hub CSPM의 계정입니다.

계정은 다음 방법 중 하나로 관리자 계정이 됩니다.

- 계정이 Security Hub CSPM에서 다른 계정에 연결되도록 해당 계정을 초대합니다. 해당 계정이 초대를 수락하면 이 계정이 멤버 계정이 되고 초대한 계정은 이들의 관리자 계정이 됩니다.
- 계정이 조직 관리 계정에 의해 Security Hub CSPM 관리자 계정으로 지정됩니다. Security Hub CSPM 관리자 계정은 모든 조직 계정을 멤버 계정으로 활성화할 수 있으며 다른 계정을 멤버 계정으로 초대할 수도 있습니다.

계정에는 관리자 계정이 하나만 있을 수 있습니다. 한 계정이 관리자 계정이면서 동시에 멤버 계정일 수 없습니다.

집계 리전

집계 리전을 설정하면 단일 창에서 여러의 보안 결과를 볼 AWS 리전 수 있습니다.

집계 리전은 사용자가 조사 결과를 보고 관리하는 리전입니다. 조사 결과는 연결된 리전의 집계 리전에 집계됩니다. 조사 결과 업데이트는 리전 전체에 복제됩니다.

집계 리전에서 보안 표준, 통찰력, 조사 결과 페이지에는 연결된 모든 리전의 데이터가 포함됩니다.

자세한 내용은 the section called “리전 간 데이터 집계” 단원을 참조하십시오.

보관된 조사 결과

레코드 상태(RecordState)가 ARCHIVED인 조사 결과입니다. 조사 결과를 보관하면 조사 결과 공급자가 해당 조사 결과가 더 이상 관련이 없다고 판단한다는 의미입니다. 레코드 상태는 조사 결과에 대한 조사의 상태를 추적하는 워크플로 상태와는 다릅니다.

조사 결과 공급자는 Security Hub CSPM API의 BatchImportFindings 작업을 사용하여 자신이 생성한 조사 결과를 보관할 수 있습니다. Security Hub CSPM은 특정 기준을 충족하는 제어 조사 결과를 자동으로 보관합니다. 자세한 내용은 제어 조사 결과 생성, 업데이트 및 보관 단원을 참조하십시오.

Security Hub CSPM 콘솔의 기본 필터 설정은 조사 결과 목록 및 테이블에서 보관된 결과를 제외합니다. 보관된 조사 결과를 포함하도록 설정을 업데이트할 수 있습니다. Security Hub CSPM API의 GetFindings 작업을 사용하여 조사 결과를 검색하면 작업은 보관된 조사 결과와 활성 조사 결과를 모두 검색합니다. 보관된 조사 결과를 제외하려면 결과를 필터링하면 됩니다. 예제:

```
"RecordState": [
    {
        "Comparison": "EQUALS",
        "Value": "ARCHIVED"
    }
],
```

AWS 보안 조사 결과 형식(ASFF)

Security Hub CSPM이 집계하거나 생성하는 조사 결과 콘텐츠의 표준화된 형식입니다. AWS Security Finding 형식을 사용하면 Security Hub CSPM을 사용하여 AWS 보안 서비스, 타사 솔루션 또는 Security Hub CSPM 자체에서 생성된 결과를 보고 분석하여 보안 검사를 실행할 수 있습니다. 자세한 내용은 AWS 보안 조사 결과 형식(ASFF) 단원을 참조하십시오.

컨트롤

정보의 기밀성, 무결성 및 가용성을 보호하고 정의된 보안 요구 사항을 충족하도록 설계된 정보 시스템 또는 조직에 대해 규정된 보호 조치 또는 대책입니다. 보안 표준은 제어 기능의 모음과 연관되어 있습니다.

보안 제어 기능이라는 용어는 표준 전반에서 단일 제어 ID와 제목을 가지고 있는 제어 기능을 말합니다. 표준 제어 기능이라는 용어는 표준별 제어 ID와 제목을 가지고 있는 제어 기능을 말합니다. 현재 Security Hub CSPM은 중국 리전 및 AWS GovCloud (US) Regions에서는 표준 제어만 지원합니다. 보안 제어 기능은 다른 모든 리전에서 지원됩니다.

사용자 지정 작업

선택한 조사 결과를 EventBridge에 전송하기 위한 Security Hub CSPM 메커니즘입니다. 사용자 지정 작업은 Security Hub CSPM에서 생성됩니다. 그런 다음에는 EventBridge 규칙에 연결됩니다. 이 규칙은 사용자 지정 작업 ID와 연결된 조사 결과가 수신될 때 수행할 특정 작업을 정의합니다. 예를 들어, 사용자 지정 작업을 사용하여 특정 조사 결과 또는 작은 조사 결과 집합을 응답 또는 수정 작업 흐름에 보낼 수 있습니다. 자세한 내용은 the section called “사용자 지정 작업 생성” 섹션을 참조하세요.

위임된 관리자 계정(조직)

에서 서비스의 AWS Organizations위임된 관리자 계정은 조직의 서비스 사용을 관리할 수 있습니다.

Security Hub CSPM에서 Security Hub CSPM 관리자 계정은 Security Hub CSPM의 위임된 관리자 계정이기도 합니다. 조직 관리 계정이 Security Hub CSPM 관리자 계정을 처음 지정하면 Security Hub CSPM이 조직을 직접적으로 호출하여 해당 계정을 위임된 관리자 계정으로 설정합니다.

그런 다음에는 조직 관리 계정이 모든 리전에서 Security Hub CSPM 관리자 계정으로 위임된 관리자 계정을 선택해야 합니다.

조사 결과

보안 점검 또는 보안 관련 감지의 관찰 가능한 기록입니다. Security Hub CSPM은 제어에 대한 보안 검사를 완료한 후 조사 결과를 생성하고 업데이트합니다. 이를 제어 조사 결과라고 합니다. 조사 결과는 다른 AWS 서비스 및 타사 제품과의 통합에서도 얻을 수 있습니다.

자세한 내용은 the section called “조사 결과” 단원을 참조하십시오.

교차 리전 집계 활성화

연결된 리전의 조사 결과, 통찰력, 제어 기능 규정 준수 상태, 보안 점수를 집계 리전으로 집계합니다. 그런 다음에는 집계 리전에서 모든 데이터를 보고 집계 리전에서 조사 결과 및 통찰력을 업데이트할 수 있습니다.

자세한 내용은 the section called “리전 간 데이터 집계” 단원을 참조하십시오.

조사 결과 수집

다른 AWS 서비스 및 타사 파트너 공급자에서 Security Hub CSPM으로 조사 결과를 가져옵니다.

조사 결과 수집 이벤트에는 새로운 조사 결과와 기존의 조사 결과에 대한 업데이트가 모두 포함됩니다.

인사이트

집계 설명 및 선택적 필터로 정의된 관련 조사 결과의 모음입니다. 인사이트는 주의와 개입이 필요한 보안 영역을 식별합니다. Security Hub CSPM은 수정할 수 없는 몇 가지 관리형(기본) 인사이트를 제공합니다. 사용자 지정 Security Hub CSPM 인사이트를 생성하여 AWS 환경 및 사용량에 고유한 보안 문제를 추적할 수도 있습니다. 자세한 내용은 the section called “인사이트” 단원을 참조하십시오.

연결된 리전

교차 리전 집계를 활성화하면, 연결된 리전은 조사 결과, 통찰력, 제어 기능 규정 준수 상태, 보안 점수를 집계 리전으로 집계하는 리전입니다.

연결된 리전에서 조사 결과 및 통찰력 페이지에는 해당 리전의 조사 결과만 포함됩니다.

자세한 내용은 the section called “리전 간 데이터 집계” 단원을 참조하십시오.

멤버 계정

관리자 계정에 조사 결과를 보고 조치를 취할 수 있는 권한을 부여한 계정입니다.

계정은 다음 방법 중 하나로 멤버 계정이 됩니다.

- 이 계정은 다른 계정의 초대를 수락합니다.
- 조직 계정의 경우, Security Hub CSPM 관리자 계정이 이 계정을 멤버 계정으로 활성화합니다.

관련 요구 사항

제어에 매핑되는 일련의 업계 또는 규정 요구 사항입니다.

규칙

제어의 준수 여부를 평가하는 데 사용되는 자동화된 기준 세트입니다. 규칙이 평가되면 통과하거나 실패할 수 있습니다. 평가에서 규칙의 통과 여부를 확인할 수 없는 경우, 규칙이 경고 상태에 있는 것입니다. 규칙을 평가할 수 없는 경우, 사용할 수 없는 상태입니다.

보안 점검

단일 리소스에 대한 규칙의 특정 시점 평가로, `PASSED`, `FAILED`, `WARNING`, 또는 `NOT_AVAILABLE` 상태의 결과를 얻습니다. 보안 점검을 실행하면 조사 결과가 생성됩니다.

Security Hub CSPM 관리자 계정

조직의 Security Hub CSPM 멤버십을 관리하는 조직 계정입니다.

조직 관리 계정은 각 리전에 있는 Security Hub CSPM 관리자 계정을 지정합니다. 조직 관리 계정은 모든 리전에서 동일한 Security Hub CSPM 관리자 계정을 선택해야 합니다.

Security Hub CSPM 관리자 계정은 조직에서 Security Hub CSPM에 대해 위임된 관리자 계정이기도 합니다.

Security Hub CSPM 관리자 계정은 어떤 조직 계정이든 멤버 계정으로 활성화할 수 있습니다. Security Hub CSPM 관리자 계정은 다른 계정을 멤버 계정으로 초대할 수도 있습니다.

보안 표준

규정 준수를 위해 충족시키거나 달성해야 하는 특성(일반적으로 측정 가능하고 제어 형식을 취함)을 명시한, 주제에 대해 게시된 진술입니다. 보안 표준은 규제 프레임워크, 모범 사례 또는 사내 정책을 기반으로 할 수 있습니다. 제어는 Security Hub CSPM에서 지원되는 하나 이상의 표준과 연결될 수 있습니다. Security Hub CSPM의 보안 표준에 대한 자세한 내용은 Security Hub CSPM의 보안 표준 이해 섹션을 참조하세요.

심각도

Security Hub CSPM 제어에 할당된 심각도는 해당 제어의 중요성을 식별합니다. 제어 기능의 심각도는 심각, 높음, 중간, 낮음 또는 정보일 수 있습니다. 제어 기능의 조사 결과에 할당된 심각도는 해당 제어 기능 자체의 심각도와 동일합니다. Security Hub CSPM이 제어에 심각도를 할당하는 방법에 대한 자세한 내용은 제어 조사 결과의 심각도 수준 섹션을 참조하세요.

워크플로 상태

결과에 대한 조사의 상태입니다. 이 상태는 `Workflow.Status` 속성을 사용하여 추적합니다.

워크플로 상태는 초기에 `NEW`입니다. 리소스 소유자에게 조사 결과에 대한 작업을 수행하도록 통지한 경우, 워크플로 상태를 `NOTIFIED`(으)로 설정할 수 있습니다. 조사 결과가 문제가 아니고 작업이 필요하지 않은 경우, 워크플로 상태를 `SUPPRESSED`(으)로 설정합니다. 조사 결과를 검토하고 수정한 후 워크플로 상태를 `RESOLVED`(으)로 설정합니다.

기본적으로 대부분의 조사 결과 목록에는 워크플로 상태가 `NEW` 또는 `NOTIFIED`인 조사 결과만 포함됩니다. 컨트롤에 대한 조사 결과 목록에는 `RESOLVED` 조사 결과도 포함됩니다.

GetFindings 작업의 경우, 워크플로 상태에 대한 필터를 포함할 수 있습니다.

```
"WorkflowStatus": [
    {
        "Comparison": "EQUALS",
        "Value": "RESOLVED"
    }
],
```

Security Hub CSPM 콘솔은 조사 결과에 대한 워크플로 상태를 설정하는 옵션을 제공합니다. 고객(또는 고객을 대신해 조사 결과 공급자의 조사 결과를 업데이트하기 위해 작업하는 SIEM, 티켓팅, 인시던트 관리 또는 SOAR 도구)도 BatchUpdateFindings을(를) 사용하여 워크플로 상태를 업데이트할 수 있습니다.

# Security Hub CSPM 활성화

AWS Security Hub CSPM을 활성화하는 방법에는 AWS Organizations 또는와 수동으로 통합하여 두 가지가 있습니다.

다중 계정 및 다중 리전 환경을 위해 Organizations과의 통합을 권장합니다. 독립형 계정이 있는 경우, Security Hub CSPM을 수동으로 설정해야 합니다.

## 필요한 권한 확인

Amazon Web Services(AWS)에 가입한 후 해당 기능을 사용하려면 Security Hub CSPM을 활성화해야 합니다. Security Hub CSPM을 활성화하려면 먼저 Security Hub CSPM 콘솔 및 API 작업에 액세스할 수 있는 권한을 설정해야 합니다. 사용자 또는 AWS 관리자는 AWS Identity and Access Management (IAM)을 사용하여 라는 관리형 정책을 IAM 자격 증명`AWSSecurityHubFullAccess`에 연결하여 AWS 이 작업을 수행할 수 있습니다.

Organizations 통합을 통해 Security Hub CSPM을 활성화하고 관리하려면 라는 AWS 관리형 정책도 연결해야 합니다`AWSSecurityHubOrganizationsAccess`.

자세한 내용은 AWS Security Hub에 대한 관리형 정책 단원을 참조하십시오.

## Organizations 통합을 통해 Security Hub CSPM 활성화

에서 Security Hub CSPM 사용을 시작하려면 조직의 AWS Organizations AWS Organizations 관리 계정이 계정을 조직의 위임된 Security Hub CSPM 관리자 계정으로 지정합니다. Security Hub CSPM은 현재 리전의 위임된 관리자 계정에서 자동으로 활성화됩니다.

원하는 방법을 선택하고 단계에 따라 위임된 관리자를 지정합니다.

Security Hub CSPM console

온보딩 시 위임된 Security Hub CSPM 관리자를 지정하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.

2. Security Hub CSPM으로 이동을 선택합니다. Organizations 관리 계정에 로그인하라는 메시지가 표시됩니다.
3. 위임된 관리자 지정 페이지의 위임된 관리자 계정 섹션에서 위임된 관리자 계정을 지정합니다. 다른 AWS 보안 및 규정 준수 서비스에 설정한 것과 동일한 위임된 관리자를 선택하는 것이 좋습니다.
4. 위임된 관리자 설정을 선택합니다.

Security Hub CSPM API

Organizations 관리 계정에서 `EnableOrganizationAdminAccount` API를 호출합니다. Security Hub CSPM 위임된 관리자 계정의 AWS 계정 ID를 입력합니다.

AWS CLI

조직 관리 계정에서 `enable-organization-admin-account` 명령을 실행합니다. Security Hub CSPM 위임된 관리자 계정의 AWS 계정 ID를 입력합니다.

명령 예제:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Organizations와의 통합에 대한 자세한 내용은 Security Hub CSPM과 통합AWS Organizations 섹션을 참조하세요.

## 중앙 구성

Security Hub CSPM과 Organizations를 통합하면 중앙 구성이라는 기능을 사용하여 조직의 Security Hub CSPM을 설정하고 관리할 수 있습니다. 중앙 구성을 사용하면 관리자가 조직의 보안 적용 범위를 사용자 지정할 수 있으므로 중앙 구성 사용을 권장합니다. 적절한 경우, 위임된 관리자는 구성원 계정이 자체 보안 범위 설정을 구성하도록 허용할 수 있습니다.

중앙 구성을 통해 위임된 관리자는 계정, OU 및 AWS 리전전반에 걸쳐 Security Hub CSPM을 구성할 수 있습니다. 위임된 관리자는 구성 정책을 만들어 Security Hub CSPM을 구성합니다. 구성 정책 내에서 다음 설정을 지정할 수 있습니다.

- Security Hub CSPM의 활성화 또는 비활성화 여부
- 활성화 및 비활성화되는 보안 표준
- 활성화 및 비활성화되는 보안 제어

- 일부 제어의 파라미터를 사용자 지정할지 여부

위임된 관리자는 전체 조직에 대한 단일 구성 정책을 만들거나 다양한 계정 및 OU에 대해 서로 다른 구성 정책을 만들 수 있습니다. 예를 들어, 테스트 계정과 프로덕션 계정은 서로 다른 구성 정책을 사용할 수 있습니다.

구성 정책을 사용하는 구성원 계정 및 OU는 중앙 관리형이며 위임된 관리자만 구성할 수 있습니다. 위임된 관리자는 특정 구성원 계정과 OU를 자체 관리형으로 지정하여 구성원이 리전별로 자체 설정을 구성할 수 있도록 할 수 있습니다.

중앙 구성을 사용하지 않는 경우, 대개 각 계정 및 리전에서 개별적으로 Security Hub CSPM을 구성해야 합니다. 이를 로컬 구성이라고 합니다. 로컬 구성에서 위임된 관리자는 현재 리전의 새로운 조직 계정에서 Security Hub CSPM 및 기본 보안 표준을 자동으로 활성화할 수 있습니다. 로컬 구성은 기존 조직 계정 또는 현재 리전 이외의 리전에는 적용되지 않습니다. 또한 로컬 구성에서는 구성 정책 사용을 지원하지 않습니다.

## 수동으로 Security Hub CSPM 활성화

독립 실행형 계정이 있거나와 통합되지 않은 경우 Security Hub CSPM을 수동으로 활성화해야 합니다 AWS Organizations. 독립 실행형 계정은 AWS Organizations 와 통합할 수 없으며 수동 활성화를 사용해야 합니다.

Security Hub CSPM을 수동으로 활성화하는 경우, Security Hub CSPM 관리자 계정을 지정하고 다른 계정을 멤버 계정으로 초대합니다. 예비 구성원 계정이 관리자 계정의 초대를 수락하면 Security Hub 관리자-구성원 관계가 성립됩니다.

원하는 방법을 선택하고 단계에 따라 Security Hub CSPM을 활성화합니다. 콘솔에서 Security Hub CSPM을 활성화하면 지원되는 보안 표준을 활성화하는 옵션도 제공됩니다.

Security Hub CSPM console

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 처음에 Security Hub CSPM 콘솔을 열면 Security Hub CSPM으로 이동을 선택합니다.
3. 시작 페이지의 보안 표준 섹션에는 Security Hub CSPM에서 지원하는 보안 표준이 나열됩니다.

   표준을 활성화하려면 확인란을 선택하고, 비활성화하려면 확인란의 선택을 취소합니다.

   언제든지 표준 또는 해당 개별 제어를 활성화하거나 비활성화할 수 있습니다. 관리형 보안 표준에 대한 자세한 정보는 Security Hub CSPM의 보안 표준 이해 섹션을 참조하세요.

4. Security Hub 활성화를 선택합니다.

Security Hub CSPM API

EnableSecurityHub API를 호출합니다. API에서 Security Hub CSPM을 활성화하면 다음의 기본 보안 표준이 자동으로 활성화됩니다.

- AWS 기본 보안 모범 사례
- Center for Internet Security(CIS) AWS Foundations Benchmark v1.2.0

이러한 표준을 사용하지 않으려면 `EnableDefaultStandards`를 `false`로 설정합니다.

`Tags` 파라미터를 사용하여 허브 리소스에 태그 값을 할당할 수도 있습니다.

AWS CLI

enable-security-hub 명령을 실행합니다. 기본 표준을 활성화하려면 `--enable-default-standards`을 포함하세요. 기본 표준을 활성화하지 않으려면 `--no-enable-default-standards`을 포함하세요. 기본 보안 표준은 다음과 같습니다.

- AWS 기본 보안 모범 사례
- Center for Internet Security(CIS) AWS Foundations Benchmark v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-
standards | --no-enable-default-standards]
```

예제

```
aws securityhub enable-security-hub --enable-default-standards --tags
 '{"Department": "Security"}'
```

## 다중 계정 활성화 스크립트

> **Note**
>
> 이 스크립트 대신 중앙 구성을 사용하여 다중 계정 및 리전에서 Security Hub CSPM을 활성화하고 구성하는 것이 좋습니다.

GitHub의 Security Hub CSPM 다중 계정 활성화 스크립트를 사용하면 계정 및 리전 전체에서 Security Hub CSPM을 활성화할 수 있습니다. 또한 이 스크립트는 구성원 계정에 초대를 보내고 AWS Config을 활성화하는 프로세스를 자동화합니다.

스크립트는 모든 리전에서 글로벌 AWS Config 리소스를 포함한 모든 리소스에 대한 리소스 기록을 자동으로 활성화합니다. 글로벌 리소스 기록을 단일 리전으로 제한하지 않습니다. 비용을 절약하려면 단일 리전에서만 글로벌 리소스를 기록하는 것이 좋습니다. 중앙 구성 또는 교차 리전 집계를 사용할 때는 이 리전이 홈 리전이어야 합니다. 자세한 내용은 에서 리소스 기록 AWS Config 단원을 참조하십시오.

여러 계정 및 리전에서 Security Hub CSPM을 비활성화하는 해당 스크립트가 있습니다.

## 다음 단계: 태세 관리 및 통합

Security Hub CSPM을 활성화한 후에는 보안 표준 및 제어를 활성화하여 보안 태세를 모니터링하는 것이 좋습니다. 제어를 활성화하면 Security Hub CSPM은 보안 검사를 실행하고 AWS 환경에서 잘못된 구성을 감지하는 데 도움이 되는 제어 조사 결과를 생성하기 시작합니다. 제어 조사 결과를 수신하려면 Security Hub CSPM AWS Config 에 대해를 활성화하고 구성해야 합니다. 자세한 내용은 Security Hub CSPM AWS Config 에 대한 활성화 및 구성 단원을 참조하십시오.

Security Hub CSPM을 활성화한 후 Security Hub CSPM과 기타 AWS 서비스 및 타사 솔루션 간의 통합을 활용하여 Security Hub CSPM에서 결과를 확인할 수도 있습니다. Security Hub CSPM은 다양한 소스로부터 일관된 형식으로 조사 결과를 수집 및 집계합니다. 자세한 내용은 Security Hub CSPM의 통합 이해 단원을 참조하십시오.

## Security Hub CSPM AWS Config 에 대한 활성화 및 구성

AWS Security Hub CSPM은 AWS Config 규칙을 사용하여 보안 검사를 실행하고 대부분의 제어에 대한 조사 결과를 생성합니다.는의 AWS 리소스 구성에 대한 자세한 보기를 AWS Config 제공합니다 AWS 계정. 규칙을 사용하여 리소스의 기준 구성을 설정하고 구성 레코더를 사용하여 특정 리소스가 규칙 조건을 위반하는지 여부를 탐지합니다.

AWS Config 관리형 규칙이라고 하는 일부 규칙은에서 사전 정의 및 개발합니다 AWS Config. 다른 규칙은 Security Hub CSPM이 개발하는 사용자 지정 AWS Config 규칙입니다. Security Hub CSPM이 제어에 사용하는 AWS Config 규칙을 서비스 연결 규칙이라고 합니다. Security Hub CSPM AWS 서비스과 같은 서비스 연결 규칙을 사용하면 계정에서 AWS Config 규칙을 생성할 수 있습니다.

AWS Security Hub CSPM과 Security Hub를 모두 활성화한 경우 Security Hub CSPM은 자동으로 서비스 연결 구성 레코더를 생성하여 보안 제어를 평가합니다. 수동으로 활성화하거나 구성할 필요가 없습니다 AWS Config. 자세한 내용은 서비스 연결 구성 레코더 사용 단원을 참조하십시오.

Security Hub 없이 Security Hub CSPM을 활성화한 경우 리소스 기록을 수동으로 활성화 AWS Config 하고 켜야 합니다. 자세한 내용은 수동으로 구성 AWS Config 단원을 참조하십시오.

이 페이지에 설명된 AWS Config 사전 조건은 AWS Foundational AWS Security Best Practices 및 CIS AWS Foundations Benchmark와 같은 보안 표준에만 적용됩니다. CIS Azure Foundations Benchmark v4.0.0과 같은 멀티클라우드 표준에서는 AWS Config 레코딩을 활성화하거나 구성 레코더를 구성할 필요가 없습니다. Security Hub CSPM 멀티클라우드 커넥터는 외부 클라우드 리소스를 평가하기 위해 서비스 연결 레코더를 자동으로 설정합니다. 멀티클라우드 표준의 유일한 사전 조건은 외부 클라우드 공급자를 위한 Security Hub CSPM 커넥터입니다.

주제


- 서비스 연결 구성 레코더 사용
- 수동으로 구성 AWS Config
- Config.1 제어 이해
- 서비스 연결 규칙 생성


## 서비스 연결 구성 레코더 사용

AWS Security Hub CSPM과 Security Hub를 모두 활성화하면 Security Hub CSPM은 계정 및 리전에서 서비스 연결 구성 레코더를 자동으로 생성하고 관리합니다. 수동으로 활성화하거나 구성할 필요가 없습니다 AWS Config.

이 구성 레코더의 이름은 입니다`AWSConfigurationRecorderForSecurityHubCSPM`. Security Hub CSPM은 Security Hub CSPM과 Security Hub가 모두 활성화된 각 계정 및 리전에 해당하는 서비스 연결 구성 레코더를 생성합니다. 새 및 AWS 계정에 대해 Security Hub CSPM을 활성화하면 AWS 리전 Security Hub CSPM이 서비스 연결 구성 레코더를 자동으로 생성합니다.

Security Hub CSPM은 서비스 연결 구성 레코더의 리소스 구성을 관리하여 Security Hub에서 지원하는 제어와 연결된 모든 리소스에 대해 레코딩이 활성화되도록 합니다. 필요한 리소스 목록은 섹션을 참조하세요제어 조사 결과에 필요한 AWS Config리소스.

Security Hub CSPM이이 서비스 연결 구성 레코더를 생성할 때 Security Hub는 고객 관리형 구성 레코더를 사용하지 않습니다 AWS Config.

구성 레코더에 대한 자세한 내용은 AWS Config 개발자 안내서의 구성 레코더 작업을 참조하세요.

## 수동으로 구성 AWS Config

Security Hub 없이 Security Hub CSPM을 활성화한 경우 다음 단계가 적용됩니다. 이 경우 계정에 AWS Config 대해를 활성화하고 활성화된 컨트롤이 평가하는 리소스 유형에 대해 리소스 기록을 켜야 합니다. 이렇게 하면 Security Hub CSPM이 적절한 AWS Config 규칙을 생성하고 보안 검사를 실행하여 결과를 생성하기 시작합니다.

### 활성화 및 구성 전 고려 사항 AWS Config

Security Hub CSPM에서 제어 조사 결과를 수신하려면 Security Hub CSPM AWS 리전 이 활성화된 각의 계정에 대해를 활성화해야 AWS Config 합니다. 다중 계정 환경에 Security Hub CSPM을 사용하는 경우, 각 리전에서 관리자 계정 및 모든 멤버 계정에 대해 AWS Config 를 활성화해야 합니다.

Security Hub CSPM 표준 및 제어를 활성화하기 AWS Config 전에에서 리소스 기록을 켜는 것이 좋습니다. 이렇게 하면 제어 조사 결과가 정확한지 확인할 수 있습니다.

에서 리소스 기록을 켜려면 구성 레코더에 연결된 AWS Identity and Access Management (IAM) 역할에 리소스를 기록할 수 있는 충분한 권한이 있어야 AWS Config합니다. 또한 IAM 정책 또는 AWS Organizations 정책으로 인해가 리소스를 기록할 수 AWS Config 있는 권한이 없도록 해야 합니다. Security Hub CSPM 제어는 리소스 구성을 직접 평가하고 AWS Organizations 정책을 고려하지 않습니다. AWS Config 기록에 대한 자세한 내용은 AWS Config 개발자 안내서의 구성 레코더 작업을 참조하세요.

Security Hub CSPM에서 표준을 활성화했지만 활성화하지 않은 경우 AWS Config Security Hub CSPM은 다음 일정에 따라 서비스 연결 AWS Config 규칙을 생성하려고 시도합니다.

- 표준을 활성화한 당일.
- 표준을 활성화한 후 익일.
- 표준을 활성화한지 3일 후.
- 표준을 활성화한지 7일 후 및 이후 7일마다 계속.

중앙 구성을 사용하는 경우 Security Hub CSPM은 하나 이상의 표준을 활성화하는 구성 정책을 계정, 조직 단위(OUs) 또는 루트와 연결할 때마다 서비스 연결 AWS Config 규칙을 생성하려고 시도합니다.

### 에서 리소스 기록 AWS Config

활성화할 때 구성 레코더에서 AWS Config 기록할 AWS 리소스를 지정해야 AWS Config합니다. 구성 레코더를 사용하면 Security Hub CSPM이 서비스 연결 규칙을 통해 리소스 구성의 변경 사항을 탐지할 수 있습니다.

Security Hub CSPM이 정확한 제어 조사 결과를 생성하려면 활성화된 제어에 해당하는 리소스 유형에 대해 AWS Config 기록을 켜야 합니다. 주로 변경 트리거 일정 유형의 활성화된 제어에 리소스 기록이 필요합니다. 일정 유형이 주기적인 일부 제어에도 리소스 기록이 필요합니다. 이러한 제어 및 관련 리소스의 목록은 제어 조사 결과에 필요한 AWS Config리소스 섹션을 참조하세요.

**Warning**

Security Hub CSPM 제어에 대한 AWS Config 기록을 올바르게 구성하지 않으면 특히 다음 인스턴스에서 제어 결과가 부정확해질 수 있습니다.

- 지정된 제어에 대한 리소스를 전혀 기록하지 않았거나 해당 유형의 리소스를 생성하기 전에 리소스 기록을 비활성화했습니다. 이러한 경우, 기록을 비활성화한 후 제어 범위에서 리소스를 생성했더라도 해당 제어에 대한 `WARNING` 조사 결과를 수신하게 됩니다. 이 `WARNING` 조사 결과는 리소스의 구성 상태를 실제로 평가하지 않는 기본 조사 결과입니다.
- 특정 제어가 평가하는 리소스에 대한 기록을 비활성화합니다. 이 경우 Security Hub CSPM은 해당 제어가 새 리소스 또는 업데이트된 리소스를 평가하지 않더라도 기록을 비활성화하기 전에 생성된 제어 조사 결과를 유지합니다. 또한 Security Hub CSPM은 조사 결과의 규정 준수 상태를 `WARNING`으로 변경합니다. 이러한 보관된 조사 결과는 리소스의 현재 구성 상태를 정확하게 반영하지 않을 수 있습니다.

기본적으로는 실행 중인 AWS 리전 에서 검색하는 지원되는 모든 리전 리소스를 AWS Config 기록합니다. 모든 Security Hub CSPM 제어 조사 결과를 수신하려면 글로벌 리소스를 기록 AWS Config 하도록 도 구성해야 합니다. 비용을 절약하려면 단일 리전에서만 글로벌 리소스를 기록하는 것이 좋습니다. 중앙 구성 또는 교차 리전 집계를 사용할 때는 이 리전이 홈 리전이어야 합니다.

에서 리소스 상태의 변화에 대한 연속 기록과 일일 기록 중에서 선택할 AWS Config수 있습니다. 일일 기록을 선택하면 리소스 상태가 변경될 경우는 각 24시간이 끝날 때마다 리소스 구성 데이터를 AWS Config 전송합니다. 변경 사항이 없는 경우에는 데이터가 제공되지 않습니다. 이로 인해 24시간 기간이 완료될 때까지 변경 트리거 제어에 대한 Security Hub CSPM 조사 결과 생성이 지연될 수 있습니다.

AWS Config 레코딩에 대한 자세한 내용은 AWS Config 개발자 안내서의 AWS 리소스 레코딩을 참조하세요.

활성화 및 구성 방법 AWS Config

다음 방법 중 하나로 리소스 기록을 활성화 AWS Config 하고 활성화할 수 있습니다.

- AWS Config 콘솔 - AWS Config 콘솔을 사용하여 계정에 AWS Config 대해를 활성화할 수 있습니다. 지침은 AWS Config 개발자 안내서의 콘솔 AWS Config 로 설정을 참조하세요.
- AWS CLI 또는 SDKs- AWS Command Line Interface ()를 사용하여 계정에 AWS Config 대해를 활성화할 수 있습니다AWS CLI. 지침은 AWS Config 개발자 안내서AWS Config 의 설정을 AWS CLI 참조하세요. AWS 소프트웨어 개발 키트(SDKs)는 여러 프로그래밍 언어에서도 사용할 수 있습니다.
- CloudFormation 템플릿 - 여러 계정에 AWS Config 대해를 활성화하려면 활성화 AWS Config라는 AWS CloudFormation 템플릿을 사용하는 것이 좋습니다. 이 템플릿에 액세스하려면 AWS CloudFormation 사용 설명서의 AWS CloudFormation StackSet 샘플 템플릿을 참조하세요.

  기본적으로 이 템플릿은 IAM 글로벌 리소스의 기록을 제외합니다. 기록 비용을 절약하려면 하나의 AWS 리전 에서만 IAM 글로벌 리소스 기록을 켜야 합니다. 교차 리전 집계를 활성화한 경우에는 이 리전이 Security Hub CSPM 홈 리전이어야 합니다. 그렇지 않으면 IAM 글로벌 리소스 기록을 지원하는 Security Hub CSPM을 사용할 수 있는 모든 리전이 될 수 있습니다. StackSet 하나를 실행하여 홈 리전 또는 다른 선택한 리전에서 IAM 글로벌 리소스를 포함한 모든 리소스를 기록하는 것이 좋습니다. 그런 다음 두 번째 StackSet를 실행하여 다른 리전에서 글로벌 리소스를 제외한 모든 리소스를 기록합니다.
- GitHub 스크립트 - Security Hub CSPM은 여러 리전의 여러 계정에 AWS Config 대해 Security Hub CSPM 및를 활성화하는 GitHub 스크립트를 제공합니다. 이 스크립트는를와 통합하지 않았거나 조직에 속하지 않은 AWS Organizations일부 멤버 계정이 있는 경우에 유용합니다.

자세한 내용은 AWS Security 블로그의 Optimize AWS Config for AWS Security Hub CSPM to effective manage your cloud security 태세 블로그 게시물을 참조하세요.

비용 고려 사항

Security Hub CSPM은 AWS Config 구성 항목을 업데이트하여 `AWS::Config::ResourceCompliance` 구성 레코더 비용에 영향을 미칠 수 있습니다. AWS Config 규칙과 연결된 Security Hub CSPM 제어가 규정 준수 상태를 변경하거나, 활성화 또는 비활성화되거나, 파라미터 업데이트가 있을 때마다 업데이트가 발생할 수 있습니다. Security Hub CSPM에만 AWS Config 구성 레코더를 사용하고 다른 목적으로이 구성 항목을 사용하지 않는 경우 해당 항목에 대한 레코딩을 끄는 것이 좋습니다 AWS Config. 이렇게 하면 AWS Config 비용을 줄일 수 있습니다. Security Hub CSPM에서 보안 검사를 실행하기 위해 `AWS::Config::ResourceCompliance`를 기록할 필요는 없습니다.

리소스 기록과 관련된 비용에 대한 자세한 내용은 AWS Security Hub CSPM 요금 및 AWS Config 요금을 참조하세요.

## Config.1 제어 이해

> **Note**
>
> AWS Security Hub CSPM과 Security Hub가 모두 활성화된 경우 Config.1 제어의 상태는 항상 입니다PASSED. Security Hub CSPM은 서비스 연결 구성 레코더를 통해 구성 항목에 직접 액세스할 수 있습니다. 자세한 내용은 서비스 연결 구성 레코더 사용 단원을 참조하십시오.

Security Hub CSPM에서 Config.1 제어는 AWS Config 가 비활성화된 경우 계정에 FAILED 조사 결과를 생성합니다. 또한 AWS Config 가 활성화되어 있지만 리소스 레코딩이 켜져 있지 않은 경우에도 계정에 FAILED 조사 결과가 생성됩니다.

AWS Config 이 활성화되어 있고 리소스 기록이 켜져 있지만 활성화된 제어가 확인하는 리소스 유형에 대해 리소스 기록이 켜져 있지 않은 경우 Security Hub CSPM은 Config.1 제어에 대한 FAILED 결과를 생성합니다. 이 FAILED 조사 결과 외에도 Security Hub CSPM은 활성화된 제어 및 해당 제어가 확인하는 리소스 유형에 대해 WARNING 조사 결과를 생성합니다. 예를 들어 KMS.5 제어를 활성화하고 리소스 레코딩이 켜져 있지 않은 경우 AWS KMS keys Security Hub CSPM은 Config.1 제어에 대한 FAILED 결과를 생성합니다. Security Hub CSPM은 KMS.5 제어 및 KMS 키에 대해서도 WARNING 조사 결과를 생성합니다.

Config.1 제어에 대한 PASSED 조사 결과를 수신하려면 활성화된 제어에 해당하는 모든 리소스 유형에 대해 리소스 기록을 켭니다. 또한 조직에 필요하지 않은 제어를 비활성화합니다. 이렇게 하면 보안 제어 검사에서 구성 격차를 없앨 수 있습니다. 또한 잘못 구성된 리소스에 대한 정확한 조사 결과를 수신할 수 있습니다.

조직의 위임된 Security Hub CSPM 관리자인 경우 해당 계정 및 멤버 계정에 대해 AWS Config 기록이 올바르게 구성되어야 합니다. 교차 리전 집계를 사용하는 경우 홈 리전 및 연결된 모든 리전에서 AWS Config 레코딩을 올바르게 구성해야 합니다. 글로벌 리소스는 연결된 리전에서 기록할 필요가 없습니다.

### 서비스 연결 규칙 생성

서비스 연결 AWS Config 규칙을 사용하는 모든 제어에 대해 Security Hub CSPM은 AWS 환경에 필요한 규칙의 인스턴스를 생성합니다.

이러한 서비스 연결 규칙은 Security Hub CSPM에 특정합니다. 동일한 규칙의 다른 인스턴스가 이미 존재하는 경우에도 Security Hub CSPM은 이러한 서비스 연결 규칙을 생성합니다. 서비스 연결 규칙은 원래 규칙 이름 앞에 securityhub를 추가하고 규칙 이름 뒤에 고유한 식별자를 추가합니다. 예를 들

어 AWS Config 관리형 규칙의 경우 `vpc-flow-logs-enabled`서비스 연결 규칙 이름은 일 수 있습니다`securityhub-vpc-flow-logs-enabled-12345`.

제어를 평가하는 데 사용할 수 있는 AWS Config 관리형 규칙 수에는 할당량이 있습니다. Security Hub CSPM이 생성하는 AWS Config 규칙은 해당 할당량에 포함되지 않습니다. 계정의 관리형 규칙 AWS Config 할당량에 이미 도달한 경우에도 보안 표준을 활성화할 수 있습니다. AWS Config 규칙 할당량에 대한 자세한 내용은 AWS Config 개발자 안내서의 에 대한 서비스 제한을 AWS Config 참조하세요.

> **Note**
>
> Security Hub CSPM 및 Security Hub를 사용하는 경우에서 서비스 연결 규칙을 볼 수 AWS Config 있지만 규칙과 연결된 규정 준수 또는 규정 미준수 리소스는 볼 수 없습니다. 규정 준수 및 규정 미준수 리소스는 Security Hub CSPM 및 Security Hub에서만 볼 수 있습니다.

## Security Hub CSPM의 로컬 구성 이해

로컬 구성은 Security Hub CSPM에서 AWS조직을 구성하는 기본 방법입니다. 중앙 구성에 옵트인하지 않고 활성화하지 않으면 조직은 기본적으로 로컬 구성을 사용합니다.

로컬 구성에서 위임된 Security Hub CSPM 관리자 계정은 구성 설정을 제한적으로 제어할 수 있습니다. 위임된 관리자가 실행할 수 있는 유일한 설정은 새로운 조직 계정에서 Security Hub CSPM 및 기본 보안 표준을 자동으로 활성화하는 것입니다. 이러한 설정은 사용자가 위임된 관리자 계정을 지정한 리전에만 적용됩니다. 기본 보안 표준은 AWSFoundational Security Best Practices(FSBP) 및 Center for Internet Security(CIS)AWSFoundations Benchmark v1.2.0입니다. 로컬 구성 설정은 기존 조직 계정 또는 위임된 관리자 계정이 지정된 리전 이외의 리전에는 적용되지 않습니다.

단일 리전의 새로운 조직 계정에서 Security Hub CSPM 및 기본 표준을 활성화하는 것 외에도 각 리전 및 계정에서 표준 및 제어를 포함하는 다른 Security Hub CSPM 설정을 구성해야 합니다. 이는 중복 프로세스가 될 수 있으므로 다음 중 하나 이상이 적용되는 경우, 다중 계정 환경에서는 중앙 구성을 사용하는 것이 좋습니다.

- 조직의 다양한 부분에 대해 서로 다른 구성 설정을 하는 것이 좋습니다(예제: 각 팀에 대해 서로 다른 활성화된 표준 또는 제어).
- 여러 리전에서 작업하면서 이러한 리전에서 서비스를 구성하는 데 드는 시간과 복잡성을 줄이기를 원할 것입니다.
- 새로운 계정이 조직에 가입할 때 특정 구성 설정을 사용하는 것이 좋습니다.
- 조직 계정이 상위 계정 또는 루트에서 특정 구성 설정을 상속하도록 하는 것이 좋습니다.

중앙 구성에 대한 자세한 내용은 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

## Security Hub CSPM의 중앙 구성 이해

중앙 구성은 여러 AWS 계정 및에서 AWS Security Hub CSPM을 설정하고 관리하는 데 도움이 되는 Security Hub CSPM 기능입니다 AWS 리전. 중앙 구성을 사용하려면 먼저 Security Hub CSPM과를 통합해야 합니다 AWS Organizations. 조직을 만들고 조직에 위임된 Security Hub CSPM 관리자 계정을 지정하여 서비스를 통합할 수 있습니다.

위임된 Security Hub CSPM 관리자 계정에서 여러 리전에 걸쳐 조직의 계정 및 조직 단위(OU)에 대해 Security Hub CSPM을 활성화할 수 있습니다. 여러 리전에 걸쳐 계정 및 OU에 대해 개별 보안 표준 및 보안 제어를 활성화, 구성, 비활성화할 수도 있습니다. 홈 리전이라고 하는 하나의 기본 리전에서 몇 단계만 거치면 이러한 설정을 구성할 수 있습니다.

중앙 구성을 사용하는 경우, 위임된 관리자는 구성할 계정과 OU를 선택할 수 있습니다. 위임된 관리자가 구성원 계정 또는 OU를 자체 관리형으로 지정하는 경우, 구성원은 각 리전에서 개별적으로 자체 설정을 구성할 수 있습니다. 위임된 관리자가 구성원 계정 또는 OU를 중앙 관리형으로 지정하는 경우, 위임된 관리자만 여러 리전에 걸쳐 구성원 계정 또는 OU를 구성할 수 있습니다. 조직의 모든 계정과 OU를 중앙 관리형, 자체 관리형 또는 이 둘의 조합으로 지정할 수 있습니다.

중앙 관리형 계정을 구성하기 위해 위임된 관리자는 Security Hub CSPM 구성 정책을 사용합니다. 위임된 관리자는 구성 정책을 통해 Security Hub CSPM의 활성화 또는 비활성화 여부와 활성화 또는 비활성화되는 표준 및 제어를 지정할 수 있습니다. 구성 정책은 특정 제어의 파라미터를 사용자 지정하는 데에도 사용할 수 있습니다.

구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 위임된 관리자는 중앙 구성을 사용하기 전에 조직의 홈 리전과 연결된 리전을 지정합니다. 연결된 리전 지정은 선택 사항입니다. 위임된 관리자는 전체 조직을 위한 단일 구성 정책을 만들거나 여러 구성 정책을 만들어 여러 계정 및 OU에 대한 변수 설정을 구성할 수 있습니다.

> **Tip**
>
> 중앙 구성을 사용하지 않는 경우, 대개 각 계정 및 리전에서 개별적으로 Security Hub CSPM을 구성해야 합니다. 이를 로컬 구성이라고 합니다. 로컬 구성에서 위임된 관리자는 현재 리전의 새로운 조직 계정에서 Security Hub CSPM 및 기본 보안 표준을 자동으로 활성화할 수 있습니다. 로컬 구성은 기존 조직 계정 또는 현재 리전 이외의 리전에는 적용되지 않습니다. 또한 로컬 구성에서는 구성 정책 사용을 지원하지 않습니다.

이 섹션에서는 중앙 구성의 개요를 다룹니다.

## 중앙 구성의 이점

중앙 구성의 이점은 다음과 같습니다.

Security Hub CSPM 서비스 및 기능의 구성 간소화

중앙 구성을 사용하는 경우, Security Hub CSPM은 조직의 보안 모범 사례를 구성하는 프로세스를 안내합니다. 또한 결과 구성 정책을 지정된 계정 및 OU에 자동으로 배포합니다. 새로운 보안 제어 자동 활성화와 같은 기존 Security Hub CSPM 설정이 있는 경우, 해당 설정을 구성 정책의 시작점으로 사용할 수 있습니다. 또한 Security Hub CSPM 콘솔의 구성 페이지에는 구성 정책, 각 정책을 사용하는 계정 및 OU에 대한 실시간 요약이 표시됩니다.

계정 및 리전 전반에 걸쳐 구성

중앙 구성을 사용하여 여러 계정 및 리전에 걸쳐 Security Hub CSPM을 구성할 수 있습니다. 이렇게 하면 조직의 각 부분이 일관된 구성과 적절한 보안 범위를 유지할 수 있습니다.

계정과 OU마다 서로 다른 구성 수용

중앙 구성을 사용하면 조직의 계정과 OU를 다양한 방식으로 구성하도록 선택할 수 있습니다. 예를 들어, 테스트 계정과 프로덕션 계정에는 서로 다른 구성이 필요할 수 있습니다. 새로운 계정이 조직에 가입할 때 적용되는 구성 정책을 만들 수도 있습니다.

구성 드리프트 방지

구성 드리프트는 사용자가 위임된 관리자의 선택 사항과 충돌하는 서비스나 기능을 변경할 때마다 발생합니다. 중앙 구성은 이러한 드리프트를 방지합니다. 계정이나 OU를 중앙 관리형으로 지정하면 조직의 위임된 관리자만 해당 계정이나 OU를 구성할 수 있습니다. 특정 계정이나 OU에서 자체 설정을 구성하도록 하려면 해당 계정이나 OU를 자체 관리형으로 지정할 수 있습니다.

## 중앙 구성을 사용해야 하는 경우

중앙 구성은 여러 Security Hub CSPM 계정이 포함된 AWS 환경에 가장 유용합니다. 이 서비스는 여러 계정의 Security Hub CSPM을 중앙에서 관리할 수 있도록 설계되었습니다.

중앙 구성을 사용하여 Security Hub CSPM 서비스, 보안 표준 및 보안 제어를 구성할 수 있습니다. 또한 이를 사용하여 특정 제어의 파라미터를 사용자 지정할 수 있습니다. 보안 표준에 대한 자세한 정보는 Security Hub CSPM의 보안 표준 이해 섹션을 참조하세요. 보안 구성에 대한 자세한 내용은 Security Hub CSPM의 보안 제어 이해 섹션을 참조하세요.

# 중앙 구성 용어 및 개념

다음 주요 용어 및 개념을 이해하면 Security Hub CSPM 중앙 구성을 사용하는 데 도움이 될 수 있습니다.

중앙 구성

조직의 위임된 Security Hub CSPM 관리자 계정이 여러 계정 및 리전에 걸쳐 Security Hub CSPM 서비스, 보안 표준 및 보안 제어를 구성하는 데 도움이 되는 Security Hub CSPM 기능입니다. 이러한 설정을 구성하기 위해 위임된 관리자는 조직의 중앙 관리형 계정에 대한 Security Hub CSPM 구성 정책을 만들고 관리합니다. 자체 관리형 계정은 각 리전에서 개별적으로 자체 설정을 구성할 수 있습니다. 중앙 구성을 사용하려면 Security Hub CSPM과를 통합해야 합니다 AWS Organizations.

홈 리전

위임된 관리자가 구성 정책을 생성하고 관리하여 Security Hub CSPM을 중앙 AWS 리전 에서 구성하는 입니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다.

홈 리전은 Security Hub CSPM 집계 영역 역할도 하며 연결된 리전으로부터 조사 결과, 인사이트 및 기타 데이터를 수신합니다.

2019년 3월 20일 이후에 AWS 도입된 리전을 옵트인 리전이라고 합니다. 옵트인 리전은 홈 리전이 될 수 없고 연결된 리전일 수 있습니다. 옵트인 리전 목록은 AWS 계정 관리 참조 안내서의 리전 활성화 및 비활성화 전 고려 사항을 참조하세요.

연결된 리전

홈 리전에서 구성할 수 AWS 리전 있는 입니다. 구성 정책은 홈 리전의 위임된 관리자가 생성합니다. 이 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 연결된 리전 지정은 선택 사항입니다.

또한 연결된 리전은 결과, 인사이트 및 기타 데이터를 홈 리전으로 보냅니다.

2019년 3월 20일 이후에 AWS 도입된 리전을 옵트인 리전이라고 합니다. 구성 정책을 적용하려면 먼저 계정에 대해 해당 리전을 활성화해야 합니다. Organizations 관리 계정은 구성원 계정의 옵트인 리전을 활성화할 수 있습니다. 자세한 내용은 계정 AWS 관리 참조 안내서의 계정에서 사용할 수 있는 지정을 참조 AWS 리전하세요.

대상

AWS 계정조직 단위(OU) 또는 조직 루트.

Security Hub CSPM 구성 정책

위임된 관리자가 중앙 관리형 계정에 대해 구성할 수 있는 Security Hub CSPM 설정 모음입니다. 여기에는 다음이 포함됩니다.

- Security Hub CSPM을 활성화 또는 비활성화할지 여부.
- 하나 이상의 보안 표준을 사용할지 여부.
- 활성화된 표준 전반에서 활성화할 보안 제어. 위임된 관리자가 활성화해야 하는 특정 제어 목록을 제공하여 이 작업을 수행할 수 있으며, Security Hub CSPM은 다른 모든 제어(새로운 제어가 릴리스된 경우 포함)를 비활성화합니다. 또는 위임된 관리자가 비활성화해야 하는 특정 제어 목록을 제공할 수 있으며, Security Hub CSPM은 다른 모든 제어(새로운 제어가 릴리스된 경우 포함)를 활성화합니다.
- 사용 가능한 표준에서 사용할 수 있는 제어를 선택할 수 있도록 파라미터를 사용자 지정할 수도 있습니다.

구성 정책은 하나 이상의 계정, OU(조직 단위) 또는 루트와 연결된 후 홈 리전 및 연결된 모든 리전에 적용됩니다.

Security Hub CSPM 콘솔에서 위임된 관리자는 Security Hub CSPM 권장 구성 정책을 선택하거나 사용자 지정 구성 정책을 만들 수 있습니다. Security Hub CSPM API 및 AWS CLI를 사용하면 위임된 관리자가 사용자 지정 구성 정책만 생성할 수 있습니다. 위임된 관리자는 최대 20개의 사용자 지정 구성 정책을 만들 수 있습니다.

권장 구성 정책에서는 Security Hub CSPM, AWS 기본 보안 모범 사례(FSBP) 표준, 모든 기존 및 새로운 FSBP 제어가 활성화됩니다. 파라미터를 허용하는 제어는 기본값을 사용합니다. 권장 구성 정책은 전체 조직에 적용됩니다.

조직에 다른 설정을 적용하거나 다른 계정 및 OU에 다른 구성 정책을 적용하려면 사용자 지정 구성 정책을 만드세요.

> **Note**
>
> 구성 정책은 AWS 보안 표준 및 제어만 지원합니다. CIS Azure Foundations Benchmark v4.0.0과 같은 멀티클라우드 표준 및 관련 멀티클라우드 제어는 구성 정책에 포함될 수 없습니다. 멀티클라우드 표준을 활성화하거나 구성하려면 원하는에서 직접 로컬 구성 메커니즘을 사용합니다 AWS 계정.

### 로컬 구성

Security Hub CSPM과를 통합한 후 조직의 기본 구성 유형입니다 AWS Organizations. 로컬 구성을 사용하면 위임된 관리자가 현재 리전의 새로운 조직 계정에서 Security Hub CSPM 및 기본 보안 표준을 자동으로 활성화하도록 선택할 수 있습니다. 위임된 관리자가 자동으로 기본 표준을 활성화하면 이러한 표준의 일부인 모든 제어도 새로운 조직 계정의 기본 파라미터와 함께 자동으로 활성화

됩니다. 이러한 설정은 기존 계정에는 적용되지 않으므로 계정이 조직에 가입한 후에 구성 드리프트가 발생할 수 있습니다. 기본 표준의 일부인 특정 제어를 비활성화하고 추가 표준 및 제어를 구성하는 작업은 각 계정 및 리전에서 개별적으로 수행해야 합니다.

로컬 구성에서는 구성 정책 사용을 지원하지 않습니다. 구성 정책을 사용하려면 중앙 구성으로 전환해야 합니다.

수동 계정 관리

Security Hub CSPM을와 통합하지 AWS Organizations 않거나 독립 실행형 계정이 있는 경우 각 리전에서 각 계정에 대한 설정을 별도로 지정해야 합니다. 수동 계정 관리는 구성 정책 사용을 지원하지 않습니다.

중앙 구성 API

위임된 Security Hub CSPM 관리자만 홈 리전에서 중앙 관리형 계정의 구성 정책을 관리하는 데 사용할 수 있는 Security Hub CSPM 작업입니다. 작업에는 다음이 포함됩니다.

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`
- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

계정별 API

계정별로 Security Hub CSPM, 표준 및 제어를 활성화하거나 비활성화하는 데 사용할 수 있는 Security Hub CSPM 작업입니다. 이러한 작업은 각 개별 리전에서 사용됩니다.

자체 관리형 계정은 계정별 작업을 사용하여 자체 설정을 구성할 수 있습니다. 중앙 관리형 계정은 홈 리전 및 연결된 리전에서 다음과 같은 계정별 작업을 사용할 수 없습니다. 해당 리전에서는 위임된 관리자만 중앙 구성 작업과 구성 정책을 통해 중앙 관리형 계정을 구성할 수 있습니다.

- `BatchDisableStandards`
- `BatchEnableStandards`

- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

중앙 관리형 계정의 소유자는 Security Hub CSPM API의 `Get` 또는 `Describe` 작업을 사용하여 계정 상태를 확인 가능합니다.

중앙 구성 대신 로컬 구성 또는 수동 계정 관리를 사용하는 경우, 이러한 계정별 작업을 사용할 수 있습니다.

자체 관리형 계정은 `*Invitations` 및 `*Members` 작업을 사용할 수도 있습니다. 그러나 자체 관리형 계정은 이러한 작업을 사용하지 않는 것을 권장합니다. 멤버 계정에 위임된 관리자와 다른 조직의 일부인 자체 멤버가 있는 경우, 정책 연결이 실패할 수 있습니다.

조직 단위(OU)

AWS Organizations 및 Security Hub CSPM에서 그룹의 컨테이너입니다 AWS 계정. 또한 조직 단위(OU)는 다른 OU를 포함할 수 있기 때문에 사용자는 위쪽에는 상위 OU가, 아래쪽에는 OU 가지가, 맨 끝에는 나뭇잎에 해당하는 계정이 있는 거꾸로 된 나무 형태의 계층 구조를 만들 수 있습니다. 각 OU는 정확히 하나의 상위 항목을 가질 수 있으며, 각 계정은 한 OU의 구성원만 될 수 있습니다.

AWS Organizations 또는에서 OUs 관리할 수 있습니다 AWS Control Tower. 자세한 내용은 AWS Organizations 사용 설명서의 조직 단위 관리 또는 AWS Control Tower 사용 설명서의 AWS Control Tower(으)로 조직 및 계정 관리를 참조하세요.

위임된 관리자는 구성 정책을 특정 계정 또는 OU에 연결하거나 조직의 모든 계정 및 OU를 포괄하는 루트와 연결할 수 있습니다.

중앙 관리형

위임된 관리자만 구성 정책을 사용하여 여러 리전에 걸쳐 구성할 수 있는 대상입니다.

위임된 관리자 계정은 계정을 대상을 중앙에서 관리할지 여부를 지정합니다. 위임된 관리자는 대상 상태를 중앙 관리형에서 자체 관리형으로 또는 그 반대로 변경할 수도 있습니다.

자체 관리형

자체 Security Hub CSPM 설정을 관리하는 대상입니다. 자체 관리형 계정은 계정별 작업을 사용하여 각 리전에서 개별적으로 Security Hub CSPM을 구성합니다. 이는 중앙 관리형 계정과 대조가 됩니다. 중앙 관리형 계정은 구성 정책을 통해 여러 리전의 위임된 관리자만 구성할 수 있습니다.

위임된 관리자 계정은 계정을 대상을 자체 관리할지 여부를 지정합니다. 위임된 관리자는 계정이나 대상에 자체 관리형 동작을 적용할 수 있습니다. 또는 계정 또는 OU가 상위 항목으로부터 자체 관리형 동작을 상속받을 수도 있습니다.

위임된 관리자 계정은 자체 관리형 계정일 수 있습니다. 위임된 관리자 계정은 대상의 상태를 자체 관리형에서 중앙 관리형으로 또는 그 반대 방향으로 변경할 수 있습니다.

구성 정책 연결

구성 정책과 계정, 조직 단위(OU) 또는 루트 간의 링크입니다. 정책 연결이 존재하는 경우, 계정, OU 또는 루트는 구성 정책에 정의된 설정을 사용합니다. 연결은 다음 두 경우 중 하나에 존재합니다.

- 위임된 관리자가 계정, OU 또는 루트에 구성 정책을 직접 적용하는 경우
- 계정 또는 OU가 상위 OU 또는 루트로부터 구성 정책을 상속하는 경우

연결은 다른 구성이 적용되거나 상속될 때까지 존재합니다.

적용된 구성 정책

위임된 관리자가 대상 계정, OU 또는 루트에 구성 정책을 직접 적용하는 구성 정책 연결의 한 유형입니다. 대상은 구성 정책에서 정의하는 방식으로 구성되며 위임된 관리자만 구성을 변경할 수 있습니다. 루트에 적용할 경우, 구성 정책은 적용 또는 가장 가까운 상위 항목으로부터의 상속을 통해 다른 구성을 사용하지 않는 조직 내 모든 계정과 OU에 영향을 미칩니다.

위임된 관리자는 자체 관리형 구성을 특정 계정, OU 또는 루트에 적용할 수도 있습니다.

상속된 구성 정책

계정이나 OU가 가장 가까운 상위 OU 또는 루트의 구성을 채택하는 구성 정책 연결의 한 유형입니다. 구성 정책은 계정이나 OU에 직접 적용되지 않는 경우, 가장 가까운 상위 항목의 구성을 상속합니다. 정책의 모든 요소가 상속됩니다. 즉, 계정이나 OU는 정책의 일부만 선택적으로 상속하도록 선택할 수 없습니다. 가장 가까운 상위 항목이 자체 관리형인 경우, 하위 계정 또는 OU는 상위 항목의 자체 관리형 동작을 상속합니다.

상속은 적용된 구성을 무시할 수 없습니다. 즉, 구성 정책 또는 자체 관리형 구성이 계정이나 OU에 직접 적용되는 경우, 해당 구성을 사용하며 상위 항목의 구성을 상속하지 않습니다.

루트

AWS Organizations 및 Security Hub CSPM에서 조직의 최상위 상위 노드입니다. 위임된 관리자가 루트에 구성 정책을 적용하면 해당 정책이 적용 또는 상속을 통해 다른 정책을 사용하거나 자체 관리형로 지정되지 않는 한 조직의 모든 계정 및 OU와 정책이 연결됩니다. 관리자가 루트를 자체 관

리형으로 지정하면 적용 또는 상속을 통한 구성 정책을 사용하지 않는 한 조직의 모든 계정과 OU가 자체 관리형입니다. 루트가 자체 관리형이고 현재 구성 정책이 없는 경우, 조직의 모든 새로운 계정은 현재 설정을 유지합니다.

조직에 가입하는 새로운 계정은 특정 OU에 할당되기 전까지는 루트에 속합니다. 새로운 계정이 OU에 할당되지 않은 경우, 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정하지 않는 한 루트 구성을 상속합니다.

## Security Hub CSPM에서 중앙 구성 활성화

위임된 AWSSecurity Hub CSPM 관리자 계정은 중앙 구성을 사용하여 여러 계정 및 조직 단위(OUs)에 대한 Security Hub CSPM, 표준 및 제어를 구성할 수 있습니다AWS 리전.

중앙 구성의 이점과 작동 방식에 대한 배경 정보는 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

이 섹션에서는 중앙 구성을 위한 사전 조건과 중앙 구성 사용을 시작하는 방법에 대해 설명합니다.

중앙 구성을 위한 사전 조건

중앙 구성 사용을 시작하려면 먼저 Security Hub CSPM을와 통합AWS Organizations하고 홈 리전을 지정해야 합니다. Security Hub CSPM 콘솔을 사용하는 경우, 이러한 사전 조건은 중앙 구성의 옵트인 워크플로에 포함됩니다.

Organizations과 통합

중앙 구성을 사용하려면 Security Hub CSPM과 Organizations를 통합해야 합니다.

이러한 서비스를 통합하려면 먼저 Organizations에서 조직을 만들어야 합니다. 그런 다음 Organizations 관리 계정에서 Security Hub CSPM 위임된 관리자 계정을 지정합니다. 지침은 Security Hub CSPM과 통합AWS Organizations 섹션을 참조하세요.

원하는 홈 리전에 위임된 관리자를 지정해야 합니다. 중앙 구성 사용을 시작하면 연결된 모든 리전에도 동일한 위임된 관리자가 자동으로 설정됩니다. Organizations 관리 계정은 위임된 관리자 계정으로 설정할 수 없습니다.

> **Important**
>
> 중앙 구성을 사용하는 경우, Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용하여 위임된 관리자 계정을 변경하거나 제거할 수 없습니다. Organizations 관리 계정이 AWS

OrganizationsAPIs 사용하여 Security Hub CSPM 위임된 관리자를 변경하거나 제거하는 경우 Security Hub CSPM은 자동으로 중앙 구성을 중지합니다. 구성 정책도 연결 해제되고 삭제됩니다. 구성원 계정은 위임된 관리자가 변경되거나 제거되기 전의 구성을 유지합니다.

### 홈 리전 지정

중앙 구성을 사용하려면 홈 리전을 지정해야 합니다. 홈 리전은 위임된 관리자가 조직을 구성하는 리전입니다.

> **Note**
>
> 홈 리전은 옵트인 리전으로 AWS지정된 리전일 수 없습니다. 옵트인 리전은 기본적으로 비활성화되어 있습니다. 옵트인 리전 목록은 AWS 계정 관리 참조 안내서의 리전 활성화 및 비활성화 전 고려 사항을 참조하세요.

선택적으로 홈 리전에서 구성할 수 있는 하나 이상의 연결된 리전을 지정할 수 있습니다.

위임된 관리자는 홈 리전에서만 구성 정책을 만들고 관리할 수 있습니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 이러한 리전 중 일부에만 적용되고 다른 리전에는 적용되지 않는 구성 정책을 만들 수 없습니다. 단, 전역 리소스와 관련된 제어는 예외입니다. 중앙 구성을 사용하는 경우, Security Hub CSPM은 홈 리전을 제외한 모든 리전의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 자세한 내용은 글로벌 리소스를 사용하는 제어 단원을 참조하십시오.

홈 리전은 연결된 리전으로부터 조사 결과, 인사이트 및 기타 데이터를 수신하는 Security Hub CSPM 집계 영역이기도 합니다.

교차 리전 집계를 위한 집계 영역을 이미 설정했다면 이 리전이 중앙 구성의 기본 홈 리전입니다. 중앙 구성을 사용하기 전에 현재 조사 결과 집계자를 삭제하고 원하는 홈 리전에 새로운 조사 결과 집계자를 생성하여 홈 리전을 변경할 수 있습니다. 조사 결과 집계자는 홈 리전 및 연결된 리전을 지정하는 Security Hub CSPM 리소스입니다.

홈 리전을 지정하려면 집계 영역 설정 단계를 따르세요. 이미 홈 리전이 있는 경우, GetFindingAggregator API를 호출하여 현재 연결된 리전을 포함하여 해당 리전에 대한 세부 정보를 확인할 수 있습니다.

### 중앙 구성 활성화 지침

원하는 방법을 선택하고 단계에 따라 조직의 중앙 구성을 활성화하세요.

Security Hub CSPM console

중앙 구성 활성화(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 설정 및 구성을 선택합니다. 그런 다음 중앙 구성 시작을 선택합니다.

   Security Hub CSPM에 온보딩하는 경우, Security Hub CSPM으로 이동을 선택합니다.
3. 위임된 관리자 지정 페이지에서 위임된 관리자 계정을 선택하거나 계정 ID를 입력합니다. 해당하는 경우, 다른 AWS 보안 및 규정 준수 서비스에 설정한 것과 동일한 위임된 관리자를 선택하는 것이 좋습니다. 위임된 관리자 설정을 선택합니다.
4. 조직 중앙 집중화 페이지의 리전 섹션에서 홈 리전을 선택합니다. 계속하려면 홈 리전에 로그인해야 합니다. 교차 리전 집계를 위한 집계 영역을 이미 설정한 경우, 해당 리전이 홈 리전으로 표시됩니다. 홈 리전을 변경하려면 리전 설정 편집을 선택합니다. 그런 다음 원하는 홈 리전을 선택하고 이 워크플로로 돌아갈 수 있습니다.
5. 홈 리전에 연결할 리전을 하나 이상 선택합니다. 필요에 따라 나중에 지원되는 리전을 홈 리전에 자동으로 연결할지 여부를 선택합니다. 여기서 선택한 리전은 위임된 관리자가 홈 리전에서 구성할 수 있습니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다.
6. 확인 및 계속을 선택합니다.
7. 이제 중앙 구성을 사용할 수 있습니다. 계속해서 콘솔 프롬프트에 따라 첫 번째 구성 정책을 생성합니다. 구성 정책을 아직 만들 준비가 되지 않았다면 아직 구성할 준비가 되지 않았음을 선택합니다. 나중에 탐색 창에서 설정 및 구성을 선택하여 정책을 만들 수 있습니다. 구성 정책 생성에 대한 지침은 구성 정책 생성 및 연결 섹션을 참조하세요.

Security Hub CSPM API

중앙 구성 활성화(API)

1. 위임된 관리자 계정의 보안 인증 정보를 사용하여 홈 리전에서 UpdateOrganizationConfiguration API를 호출합니다.
2. `AutoEnable` 필드를 `false`(으)로 설정합니다.
3. `OrganizationConfiguration` 객체의 `ConfigurationType` 필드를 `CENTRAL`(으)로 설정합니다. 이 작업은 다음과 같은 영향을 미칩니다.

   - 호출 계정을 연결된 모든 리전의 Security Hub CSPM 위임된 관리자로 지정합니다.
   - 연결된 모든 리전의 위임된 관리자 계정에서 Security Hub CSPM을 활성화합니다.

- 호출 계정을 Security Hub CSPM을 사용하고 조직에 속하는 새로운 및 기존 계정의 Security Hub CSPM 위임된 관리자로 지정합니다. 이는 홈 리전 및 연결된 모든 리전에서 발생합니다. 호출 계정은 Security Hub CSPM이 활성화된 구성 정책에 연결된 경우에만 새로운 조직 계정의 위임된 관리자로 설정됩니다. 호출 계정은 Security Hub CSPM이 이미 활성화된 경우에만 기존 조직 계정의 위임된 관리자로 설정됩니다.
- 연결된 모든 리전에서 AutoEnable을(를) `false`(으)로 설정하고 홈 리전 및 연결된 모든 리전에서 AutoEnableStandards을(를) `NONE`(으)로 설정합니다. 이러한 파라미터는 중앙 구성을 사용할 때 홈 리전 및 연결된 리전과 관련이 없지만 구성 정책을 사용하여 조직 계정에서 Security Hub CSPM 및 기본 보안 표준을 자동으로 활성화할 수 있습니다.

4. 이제 중앙 구성을 사용할 수 있습니다. 위임된 관리자는 조직의 Security Hub CSPM을 구성하는 구성 정책을 만들 수 있습니다. 구성 정책 생성에 대한 지침은 구성 정책 생성 및 연결 섹션을 참조하세요.

API 요청 예제:

```
{
    "AutoEnable": false,
    "OrganizationConfiguration": {
        "ConfigurationType": "CENTRAL"
    }
}
```

AWS CLI

중앙 구성 활성화(AWS CLI)

1. 위임된 관리자 계정의 보안 인증 정보를 사용하여 홈 리전에서 update-organization-configuration 명령을 실행합니다.
2. `no-auto-enable` 파라미터를 포함합니다.
3. `organization-configuration` 객체의 `ConfigurationType` 필드를 `CENTRAL`(으)로 설정합니다. 이 작업은 다음과 같은 영향을 미칩니다.

   - 호출 계정을 연결된 모든 리전의 Security Hub CSPM 위임된 관리자로 지정합니다.
   - 연결된 모든 리전의 위임된 관리자 계정에서 Security Hub CSPM을 활성화합니다.
   - 호출 계정을 Security Hub CSPM을 사용하고 조직에 속하는 새로운 및 기존 계정의 Security Hub CSPM 위임된 관리자로 지정합니다. 이는 홈 리전 및 연결된 모든 리전에서 발생합니

다. 통화 계정은 Security Hub가 활성화된 구성 정책에 연결된 경우에만 새로운 조직 계정의 위임된 관리자로 설정됩니다. 호출 계정은 Security Hub CSPM이 이미 활성화된 경우에만 기존 조직 계정의 위임된 관리자로 설정됩니다.

- 연결된 모든 리전에서 자동 활성화 옵션을 no-auto-enable로 설정하고 홈 리전 및 연결된 모든 리전에서 auto-enable-standards를 NONE으로 설정합니다. 이러한 파라미터는 중앙 구성을 사용할 때 홈 리전 및 연결된 리전과 관련이 없지만 구성 정책을 사용하여 조직 계정에서 Security Hub CSPM 및 기본 보안 표준을 자동으로 활성화할 수 있습니다.

4. 이제 중앙 구성을 사용할 수 있습니다. 위임된 관리자는 조직의 Security Hub CSPM을 구성하는 구성 정책을 만들 수 있습니다. 구성 정책 생성에 대한 지침은 구성 정책 생성 및 연결 섹션을 참조하세요.

명령 예제:

```
aws securityhub --region us-east-1 update-organization-configuration \
--no-auto-enable \
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

## 중앙 관리형 및 자체 관리형 대상

중앙 구성을 활성화하면 위임된 AWSSecurity Hub CSPM 관리자가 각 조직 계정, 조직 단위(OU) 및 루트를 중앙 관리형 또는 자체 관리형으로 지정할 수 있습니다. 대상의 관리 유형에 따라 Security Hub CSPM 설정을 지정하는 방법이 결정됩니다.

중앙 구성의 이점과 작동 방식에 대한 배경 정보는 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

이 섹션에서는 중앙 관리형 지정과 자체 관리형 지정의 차이점과 계정, OU 또는 루트의 관리 유형을 선택하는 방법을 설명합니다.

자체 관리형

자체 관리형 계정, OU 또는 루트의 소유자는 각각에서 별도로 설정을 구성해야 합니다AWS 리전. 위임된 관리자는 자체 관리형 대상에 대한 구성 정책을 생성할 수 없습니다.

중앙 관리형

위임된 Security Hub CSPM 관리자만이 홈 리전 및 연결된 리전의 중앙 관리 계정, OU 또는 루트의 설정을 구성할 수 있습니다. 구성 정책을 중앙 관리형 계정 및 OU에 연결할 수 있습니다.

위임된 관리자는 계정이나 중앙 관리 사이의 대상 상태를 전환할 수 있습니다. 기본적으로 Security Hub CSPM API를 통해 중앙 구성을 시작하면 모든 계정과 OU는 자체 관리합니다. 콘솔에서 관리 유형은 첫 번째 구성 정책에 따라 달라집니다. 첫 번째 정책에 연결하는 계정과 OU는 중앙에서 관리합니다. 다른 계정과 OU는 기본적으로 자체에서 관리합니다.

구성 정책을 이전의 자체 관리형 계정과 연결하면 정책 설정이 자체 관리형 지정을 재정의합니다. 계정이 중앙에서 관리되고 구성 정책에 반영된 설정을 채택합니다.

중앙 관리형 계정을 자체 관리형 계정으로 변경하면 이전에 구성 정책을 통해 계정에 적용된 설정이 그대로 유지됩니다. 예를 들어 중앙 관리형 계정은 처음에 Security Hub CSPM을 활성화하고AWS, 기본 보안 모범 사례를 활성화하고, CloudTrail.1. 그런 다음 이 계정을 자체 관리형으로 지정하면 모든 설정이 변경되지 않습니다. 하지만 이후 계정 소유자가 계정의 설정을 독립적으로 변경할 수 있습니다.

하위 계정과 OU는 자체 관리형 상위 계정의 자체 관리형 동작을 상속할 수 있습니다. 이는 하위 계정과 OU가 중앙 관리형 상위 계정으로부터 구성 정책을 상속받는 것과 마찬가지입니다. 자세한 내용은 적용 및 상속을 통한 정책 연결 섹션을 참조하세요.

자체 관리형 계정 또는 OU는 상위 노드 또는 루트에서 구성 정책을 상속할 수 없습니다. 예를 들어, 조직의 모든 계정과 OU가 루트에서 구성 정책을 상속하도록 하려면 자체 관리형 노드의 관리 유형을 중앙 관리형으로 변경해야 합니다.

자체 관리형 계정에서 설정을 구성하는 옵션

자체 관리형 계정은 각 리전에서 개별적으로 자체 설정을 구성해야 합니다.

자체 관리형 계정의 소유자는 각 리전에서 Security Hub CSPM API의 작업을 간접적으로 호출하여 설정을 구성할 수 있습니다.

- Security Hub CSPM 서비스를 활성화 또는 비활성화하는 `EnableSecurityHub` 및 `DisableSecurityHub`(자체 관리형 계정에 위임된 Security Hub CSPM 관리자가 있는 경우, 계정 소유자가 Security Hub CSPM을 비활성화하기 전에 관리자가 계정을 연결 해제해야 함).
- 표준을 활성화 또는 비활성화하는 `BatchEnableStandards` 및 `BatchDisableStandards`
- 제어를 활성화 또는 비활성화하는 `BatchUpdateStandardsControlAssociations` 또는 `UpdateStandardsControl`

자체 관리형 계정은 `*Invitations` 및 `*Members` 작업을 사용할 수도 있습니다. 그러나 자체 관리형 계정은 이러한 작업을 사용하지 않는 것을 권장합니다. 멤버 계정에 위임된 관리자와 다른 조직의 일부인 자체 멤버가 있는 경우, 정책 연결이 실패할 수 있습니다.

Security Hub CSPM API 작업에 대한 설명은 AWS Security Hub CSPM API 참조를 참조하세요.

자체 관리형 계정은 Security Hub CSPM 콘솔 또는를 사용하여 각 리전에서 설정을 AWS CLI구성할 수도 있습니다.

자체 관리형 계정은 Security Hub CSPM 구성 정책 및 정책 연결과 관련된 API를 간접적으로 호출할 수 없습니다. 위임된 관리자만 중앙 구성 API를 호출하고 구성 정책을 사용하여 중앙 관리형 계정을 구성할 수 있습니다.

대상의 관리 유형 선택

원하는 방법을 선택하고 단계에 따라 AWSSecurity Hub CSPM에서 계정 또는 OU를 중앙 관리형 또는 자체 관리형으로 지정합니다.

Security Hub CSPM console

계정 또는 OU의 관리 유형을 선택하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 구성을 선택합니다.
3. 조직 탭에서 대상 계정 또는 OU를 선택합니다. 편집을 선택합니다.
4. 위임된 관리자가 대상 계정 또는 OU를 구성하도록 하려면 구성 정의 페이지의 관리 유형에서 중앙 관리형을 선택합니다. 그런 다음 기존 구성 정책을 대상과 연결하려면 특정 정책 적용을 선택합니다. 대상이 가장 가까운 상위 항목의 구성을 상속하도록 하려면 나의 조직에서 상속을 선택합니다. 계정이나 OU에서 자체 설정을 구성하도록 하려면 자체 관리형을 선택합니다.
5. 다음을 선택합니다. 변경 사항을 검토하고 저장을 선택합니다.

Security Hub CSPM API

계정 또는 OU의 관리 유형을 선택하려면

1. 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 StartConfigurationPolicyAssociation API를 간접적으로 호출합니다.
2. `ConfigurationPolicyIdentifier` 필드에서 계정 또는 OU가 자체 설정을 제어하도록 하려면 `SELF_MANAGED_SECURITY_HUB`을(를) 입력합니다. 위임된 관리자가 계정 또는 OU에 대한 설정을 제어하도록 하려면 관련 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 제공합니다.

3. `Target` 필드에 관리 유형을 변경하려는 대상의 AWS 계정ID, OU ID 또는 루트 ID를 입력합니다. 그러면 자체 관리형 동작 또는 지정된 구성 정책이 대상과 연결됩니다. 대상의 하위 계정은 자체 관리형 동작 또는 구성 정책을 상속할 수 있습니다.

자체 관리형 계정을 지정하기 위한 API 요청 예제:

```
{
    "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
    "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

계정 또는 OU의 관리 유형을 선택하려면

1. 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 start-configuration-policy-association 명령을 실행합니다.
2. `configuration-policy-identifier` 필드에서 계정 또는 OU가 자체 설정을 제어하도록 하려면 `SELF_MANAGED_SECURITY_HUB`을(를) 입력합니다. 위임된 관리자가 계정 또는 OU에 대한 설정을 제어하도록 하려면 관련 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 제공합니다.
3. `target` 필드에 관리 유형을 변경하려는 대상의 AWS 계정ID, OU ID 또는 루트 ID를 입력합니다. 그러면 자체 관리형 동작 또는 지정된 구성 정책이 대상과 연결됩니다. 대상의 하위 계정은 자체 관리형 동작 또는 구성 정책을 상속할 수 있습니다.

자체 관리형 계정을 지정하기 위한 명령 예제:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \
--target '{"AccountId": "123456789012"}'
```

## Security Hub CSPM 구성 정책 작동 방식

위임된 AWS Security Hub CSPM 관리자는 구성 정책을 생성하여 조직의 Security Hub CSPM, 보안 표준 및 보안 제어를 구성할 수 있습니다. 구성 정책을 생성한 후 위임된 관리자는 이를 특정 계정, 조직 단위(OU) 또는 루트에 연결할 수 있습니다. 그러면 지정된 계정, OU 또는 루트에 정책이 적용됩니다.

중앙 구성의 이점과 작동 방식에 대한 배경 정보는 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

이 섹션에서는 구성 정책에 대한 자세한 개요를 제공합니다.

### 정책 고려 사항

Security Hub CSPM에서 구성 정책을 만들 전에 다음 사항을 고려하세요.

- 구성 정책을 적용하려면 연결해야 합니다 – 구성 정책을 만든 후 하나 이상의 계정, OU(조직 단위) 또는 루트와 연결할 수 있습니다. 구성 정책은 직접 적용을 통해 또는 상위 OU로부터의 상속을 통해 계정 또는 OU와 연결할 수 있습니다.
- 계정 또는 OU를 하나의 구성 정책에만 연결할 수 있습니다 – 설정 충돌을 방지하기 위해 계정 또는 OU를 한 번에 하나의 구성 정책에만 연결할 수 있습니다. 또는 계정이나 OU를 자체 관리할 수도 있습니다.
- 구성 정책은 완전합니다 – 구성 정책은 완전한 설정 사양을 제공합니다. 예를 들어, 하위 계정은 한 정책의 일부 제어에 대한 설정과 다른 정책의 다른 제어에 대한 설정을 수락할 수 없습니다. 정책을 하위 계정에 연결할 때는 하위 계정에서 사용할 모든 설정이 정책에 지정되어 있는지 확인하세요.
- 구성 정책은 되돌릴 수 없습니다 – 계정 또는 OU와 연결한 후에는 구성 정책을 되돌리는 옵션이 없습니다. 예를 들어, CloudWatch 제어를 비활성화하는 구성 정책을 특정 계정과 연결한 다음 해당 정책의 연결을 해제하면 해당 계정에서 CloudWatch 제어가 비활성화된 상태로 유지됩니다. CloudWatch 제어를 다시 활성화하려면 계정을 제어를 활성화하는 새로운 정책과 연결할 수 있습니다. 또는 계정을 자체 관리형으로 변경하고 계정의 각 CloudWatch 제어를 활성화할 수 있습니다.
- 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다 – 구성 정책은 홈 리전 및 연결된 모든 리전의 모든 관련 계정에 영향을 미칩니다. 이러한 리전 중 일부에만 적용되고 다른 리전에는 적용되지 않는 구성 정책을 만들 수 없습니다. 단, 글로벌 리소스와 관련된 제어는 예외입니다. Security Hub CSPM은 홈 리전을 제외한 모든 리전의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다.

  2019년 3월 20일 이후에 AWS 도입된 리전을 옵트인 리전이라고 합니다. 구성 정책이 계정에 적용되기 전에 해당 계정의 리전을 활성화해야 합니다. Organizations 관리 계정은 구성원 계정의 옵트인 리전을 활성화할 수 있습니다. 옵트인 리전 활성화에 대한 지침은 AWS 계정 관리 참조 안내서의 계정에서 사용할 수 있는 지정을 참조 AWS 리전하세요.

정책이 홈 리전 또는 하나 이상의 연결된 리전에서 사용할 수 없는 제어를 구성하는 경우, Security Hub CSPM은 사용할 수 없는 리전의 제어 구성을 건너뛰고 제어를 사용할 수 있는 리전에 구성을 적용합니다. 홈 리전 또는 연결된 리전에서 사용할 수 없는 제어에 대한 적용 범위가 부족합니다.

- 구성 정책은 리소스입니다 – 구정 정책은 리소스로서 Amazon 리소스 이름(ARN) 및 범용 고유 식별자(UUID)를 포함합니다. 제품 ARN은 `arn:`*`partition:`*`securityhub:`*`region`*`:`*`delegated administrator account ID`*`:configuration-policy/`*`configuration policy UUID`* 형식을 사용합니다. 자체 관리형 구성에는 ARN 또는 UUID가 없습니다. 자체 관리형 구성의 식별자는 `SELF_MANAGED_SECURITY_HUB`입니다.
- 멀티클라우드 표준은 구성 정책에서 지원되지 않습니다. 구성 정책에는 AWS 보안 표준 및 제어만 포함될 수 있습니다. CIS Azure Foundations Benchmark v4.0.0과 같은 멀티클라우드 표준 및 관련 제어(예: `Azure.Storage.1`)는 구성 정책에 포함될 수 없습니다. 구성 정책에 멀티클라우드 표준 ARN 또는 제어 ID를 포함하는 경우 요청은를 반환합니다`InvalidInputException`. 멀티클라우드 표준을 활성화하거나 구성하려면 원하는에서 직접 로컬 구성 메커니즘을 사용합니다 AWS 계정.

구성 정책 유형

각 구성 정책은 다음 설정을 지정합니다.

- Security Hub CSPM을 활성화하거나 비활성화합니다.
- 하나 이상의 보안 표준을 활성화합니다.
- 활성화된 표준 전반에서 어떤 보안 제어를 사용할 수 있는지 표시합니다. 이를 위해 활성화해야 하는 특정 제어 목록을 제공할 수 있습니다. 그러면 Security Hub CSPM은 새로운 제어가 릴리스될 때 새로운 제어를 포함한 다른 모든 제어를 비활성화합니다. 또는 비활성화해야 하는 특정 제어의 목록을 제공할 수 있습니다. 그러면 Security Hub CSPM은 새로운 제어가 릴리스될 때 새로운 제어를 포함한 다른 모든 제어를 활성화합니다.
- 사용 가능한 표준에서 사용할 수 있는 제어를 선택할 수 있도록 파라미터를 사용자 지정할 수도 있습니다.

중앙 구성 정책에는 AWS Config 레코더 설정이 포함되지 않습니다. Security Hub CSPM이 제어 조사 결과를 생성하려면 필요한 리소스에 대한 기록을 별도로 활성화 AWS Config 하고 활성화해야 합니다. 자세한 내용은 활성화 및 구성 전 고려 사항 AWS Config 단원을 참조하십시오.

중앙 구성을 사용하는 경우, Security Hub CSPM은 홈 리전을 제외한 모든 리전의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 활성화하도록 선택한 다른 제어는 사용 가능한 모든 리전에서 활성화됩니다. 이러한 제어에 대한 조사 결과를 한 리전으로만 제한하려면 홈 리전

을 제외한 모든 리전에서 AWS Config 레코더 설정을 업데이트하고 글로벌 리소스 기록을 끌 수 있습니다.

글로벌 리소스를 평가하는 활성화된 제어가 홈 리전에서 지원되지 않는 경우 Security Hub CSPM은 해당 제어가 지원되는 연결된 리전에서 제어를 활성화하려고 시도합니다. 중앙 구성을 사용하는 경우, 홈 리전 또는 연결된 리전에서 사용할 수 없는 제어에 대한 적용 범위가 부족합니다.

글로벌 리소스와 관련된 제어 목록은 글로벌 리소스를 사용하는 제어 섹션을 참조하세요.

권장 구성 정책

Security Hub CSPM 콘솔에서 처음으로 구성 정책을 생성할 때는 Security Hub CSPM 권장 정책을 선택할 수 있습니다.

권장 정책은 Security Hub CSPM, AWS 기본 보안 모범 사례(FSBP) 표준, 모든 기존 및 새 FSBP 제어를 활성화합니다. 파라미터를 허용하는 제어는 기본값을 사용합니다. 권장 정책은 루트(새로운 및 기존 모든 계정 및 OU)에 적용됩니다. 조직을 위한 권장 정책을 만든 후 위임된 관리자 계정에서 수정할 수 있습니다. 예를 들어, 추가 표준 또는 제어를 활성화하거나 특정 FSBP 제어를 비활성화할 수 있습니다. 구성 정책 수정에 대한 지침은 구성 정책 업데이트 섹션을 참조하세요.

사용자 지정 구성 정책

위임된 관리자는 권장 정책 대신 최대 20개의 사용자 지정 구성 정책을 만들 수 있습니다. 단일 사용자 지정 정책을 전체 조직에 연결하거나 계정 및 OU가 서로 다른 사용자 지정 정책을 연결할 수 있습니다. 사용자 지정 구성 정책에서 원하는 설정을 지정합니다. 예를 들어, FSBP, CIS(인터넷 보안 센터) AWS Foundations Benchmark v1.4.0 및 Amazon Redshift 제어를 제외한 해당 표준의 모든 제어를 활성화하는 사용자 지정 정책을 생성할 수 있습니다. 사용자 지정 구성 정책에 사용하는 세분화 수준은 조직 전체의 의도한 보안 적용 범위에 따라 달라집니다.

> **Note**
>
> Security Hub CSPM을 비활성화하는 구성 정책을 위임된 관리자 계정과 연결할 수 없습니다. 이러한 정책을 다른 계정과 연결할 수는 있지만 위임된 관리자와의 연결은 건너뜁니다. 위임된 관리자 계정은 현재의 구성을 유지합니다.

사용자 지정 구성 정책을 만든 후 권장 구성을 반영하도록 구성 정책을 업데이트하여 권장 구성 정책으로 전환할 수 있습니다. 하지만 첫 번째 정책을 만든 후에는 Security Hub CSPM 콘솔에 권장 구성 정책을 생성할 수 있는 옵션이 표시되지 않습니다.

### 적용 및 상속을 통한 정책 연결

처음에 중앙 구성을 선택하면 조직은 연결되지 않으면 옵트인 전과 동일한 방식으로 동작합니다. 그러면 위임된 관리자가 구성 정책과 자체 관리형 동작, 계정, OU 또는 루트 간에 연결을 설정할 수 있습니다. 적용 또는 상속을 통해 연결을 설정할 수 있습니다.

위임된 관리자 계정에서 구성 정책을 계정, OU 또는 루트에 직접 적용할 수 있습니다. 또는 위임된 관리자 계정, OU 또는 루트에 자체 관리형으로 직접 지정할 수도 있습니다.

직접 적용이 없는 경우, 계정 또는 OU는 구성 정책 또는 자체 관리형 동작이 있는 가장 가까운 상위 항목의 설정을 상속합니다. 가장 가까운 상위 항목이 구성 정책에 연결되어 있는 경우, 해당 정책은 해당 하위 항목에 상속되며 홈 리전의 위임된 관리자만 구성할 수 있습니다. 가장 가까운 상위가 자체 관리형인 경우 하위는 자체 관리형 동작을 상속하고 각각에 자체 설정을 지정할 수 있습니다 AWS 리전.

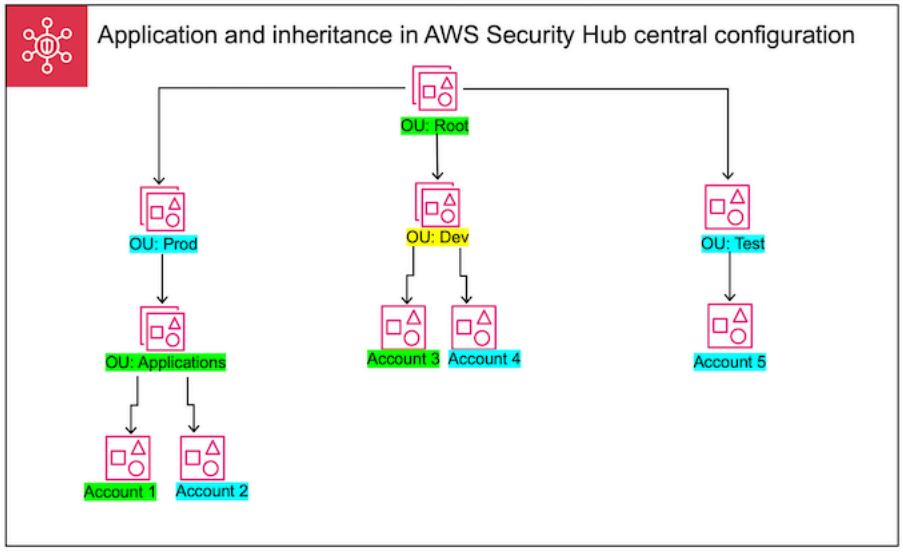
적용은 상속보다 우선합니다. 즉, 위임된 관리자가 계정이나 OU에 직접 적용한 구성 정책 또는 자체 관리형 지정은 상속이 재정의할 수 없습니다.

자체 관리형 계정에 구성 정책을 직접 적용하는 경우, 정책은 자체 관리형 지정을 재정의합니다. 계정이 중앙에서 관리되고 구성 정책에 반영된 설정을 채택합니다.

루트에 구성 정책을 직접 적용하는 것이 좋습니다. 정책을 루트에 적용하면 조직에 가입한 새로운 계정을 다른 정책에 연결하거나 자체 관리형으로 지정하지 않는 한 루트 정책을 자동으로 상속합니다.

적용이나 상속을 통해 한 번에 하나의 구성 정책만 계정이나 OU에 연결할 수 있습니다. 이는 설정 충돌을 방지하기 위한 것입니다.

다음 다이어그램은 중앙 구성에서 정책 적용 및 상속이 작동하는 방식을 보여줍니다.



이 예제에서 녹색으로 강조 표시된 노드에는 구성 정책이 적용되어 있습니다. 파란색으로 강조 표시된 노드에는 해당 노드에 적용된 구성 정책이 없습니다. 노란색으로 강조 표시된 노드는 자체 관리형 노드로 지정되었습니다. 각 계정 및 OU는 다음 구성을 사용합니다.

- OU:Root(녹색) – 이 OU는 해당 OU에 적용된 구성 정책을 사용합니다.
- OU:Prod(파란색) – 이 OU는 OU:Root의 구성 정책을 상속합니다.
- OU:Applications(녹색) – 이 OU는 해당 OU에 적용된 구성 정책을 사용합니다.
- Account 1(녹색) – 이 계정은 해당 계정에 적용된 구성 정책을 사용합니다.
- Account 2(파란색) – 이 계정은 OU:Applications의 구성 정책을 상속합니다.
- OU:Dev(노란색) – 이 OU는 자체 관리형입니다.
- Account 3(녹색) – 이 계정은 해당 계정에 적용된 구성 정책을 사용합니다.
- Account 4(파란색) – 이 계정은 OU:Dev의 자체 관리형 동작을 상속합니다.
- OU:Test(파란색) – 이 계정은 OU:Root의 구성 정책을 상속합니다.
- Account 5(파란색) – 이 계정은 OU:Root의 구성 정책을 상속합니다. 직계 상위 항목인 OU:Test가 구성 정책과 연결되어 있지 않기 때문입니다.

구성 정책 테스트

구성 정책이 작동하는 방식을 이해하려면 하나의 정책을 생성하고 이를 테스트 계정 또는 OU와 연결하는 것이 좋습니다.

구성 정책을 테스트하려면

1. 사용자 지정 구성 정책을 만들고 Security Hub CSPM 활성화, 표준 및 제어에 대해 지정된 설정이 올바른지 확인합니다. 지침은 구성 정책 생성 및 연결 섹션을 참조하세요.
2. 하위 계정이나 OU가 없는 테스트 계정 또는 OU에 구성 정책을 적용합니다.
3. 테스트 계정 또는 OU가 홈 리전 및 연결된 모든 리전에서 예상대로 구성 정책을 사용하는지 확인합니다. 또한 조직의 다른 모든 계정과 OU가 자체 관리 상태를 유지하고 각 리전에서 자체 설정을 변경할 수 있는지 확인할 수 있습니다.

단일 계정 또는 OU에서 구성 정책을 테스트한 후 다른 계정 및 OU와 연결할 수 있습니다.

## 구성 정책 생성 및 연결

위임된 AWS Security Hub CSPM 관리자 계정은 Security Hub CSPM, 표준 및 제어가 지정된 계정 및 조직 단위(OUs. 구성 정책은 위임된 관리자가 이를 적어도 하나 이상의 계정 또는 조직 단위(OU) 또는

루트에 연결한 후에만 적용됩니다. 위임된 관리자는 자체 관리형 구성을 특정 계정, OU 또는 루트에 적용할 수도 있습니다.

구성 정책을 처음 생성하는 경우, 먼저 Security Hub CSPM 구성 정책 작동 방식 섹션을 검토하는 것이 좋습니다.

> **Note**
>
> 구성 정책은 AWS 표준 및 제어만 지원합니다. 구성 정책에 멀티클라우드 표준(예: CIS Azure Foundations Benchmark v4.0.0) 또는 Azure 제어를 포함할 수 없습니다. 멀티클라우드 표준 ARN 또는 제어 ID를 포함하면가 반환됩니다`InvalidInputException`. 멀티클라우드 표준을 활성화하거나 구성하려면 원하는에서 직접 로컬 구성 메커니즘을 사용합니다 AWS 계정.

원하는 액세스 방법을 선택하고 단계에 따라 구성 정책 또는 자체 관리 구성을 만들고 연결합니다. Security Hub CSPM 콘솔을 사용하는 경우, 구성을 여러 계정 또는 OU에 동시에 적용할 수 있습니다. Security Hub CSPM API 또는를 사용하는 경우 각 요청에서 하나의 계정 또는 OU에만 구성을 연결할 AWS CLI수 있습니다.

> **Note**
>
> 중앙 구성을 사용하는 경우, Security Hub CSPM은 홈 리전을 제외한 모든 리전의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 활성화하도록 선택한 다른 제어는 사용 가능한 모든 리전에서 활성화됩니다. 이러한 제어에 대한 조사 결과를 한 리전으로만 제한하려면 홈 리전을 제외한 모든 리전에서 AWS Config 레코더 설정을 업데이트하고 글로벌 리소스 기록을 끌 수 있습니다.
>
> 글로벌 리소스를 평가하는 활성화된 제어가 홈 리전에서 지원되지 않는 경우 Security Hub CSPM은 해당 제어가 지원되는 연결된 리전에서 제어를 활성화하려고 시도합니다. 중앙 구성을 사용하는 경우, 홈 리전 또는 연결된 리전에서 사용할 수 없는 제어에 대한 적용 범위가 부족합니다.
>
> 글로벌 리소스와 관련된 제어 목록은 글로벌 리소스를 사용하는 제어 섹션을 참조하세요.

Security Hub CSPM console

구성 정책을 만들고 연결하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.

홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.

2. 탐색 창에서 구성 및 정책 탭을 선택합니다. 그런 다음 정책 생성을 선택합니다.
3. 구성 정책을 처음 만들면 조직 구성 페이지의 구성 유형 아래에 세 가지 옵션이 표시됩니다. 구성 정책을 하나 이상 이미 만든 경우, 사용자 지정 정책 옵션만 표시됩니다.

   - AWS 권장 정책을 사용하려면 전체 조직에서 권장 Security Hub CSPM 구성 사용을 선택합니다. 권장 정책은 모든 조직 계정에서 Security Hub CSPM을 활성화하고, AWS 기본 보안 모범 사례(FSBP) 표준을 활성화하며, 모든 신규 및 기존 FSBP 제어를 활성화합니다. 제어는 기본 파라미터 값을 사용합니다.
   - 나중에 구성 정책을 만들려면 아직 구성할 준비가 되지 않았음을 선택합니다.
   - 사용자 지정 정책을 선택하여 사용자 지정 구성 정책을 생성합니다. Security Hub CSPM을 활성화 또는 비활성화할지 여부, 활성화할 표준, 해당 표준에서 활성화할 제어를 지정합니다. 필요에 따라 사용자 지정 파라미터를 지원하는 하나 이상의 활성화된 제어에 대해 사용자 지정 파라미터 값을 지정합니다.
4. 계정 섹션에서 구성 정책을 적용할 대상 계정, OU 또는 루트를 선택합니다.

   - 구성 정책을 루트에 적용하려면 모든 계정을 선택합니다. 여기에는 다른 정책이 적용되거나 상속되지 않은 조직 내 모든 계정과 OU가 포함됩니다.
   - 구성 정책을 특정 계정 또는 OU에 적용하려면 특정 계정을 선택합니다. 계정 ID를 입력하거나 조직 구조에서 계정 및 OU를 선택합니다. 정책을 생성할 때 최대 15개의 대상(계정, OU 또는 루트)에 정책을 적용할 수 있습니다. 더 큰 수를 지정하려면 정책을 만든 후 편집하여 추가 대상에 적용하세요.
   - 구성 정책을 현재 위임된 관리자 계정에 적용하려면 위임된 관리자만을 선택합니다.
5. 다음을 선택합니다.
6. 검토 및 배포 페이지에서 구성 정책 세부 정보를 검토합니다. 그런 다음 정책 생성 및 연결을 선택합니다. 홈 리전 및 연결된 리전에서 이 작업은 이 구성 정책과 연결된 계정의 기존 구성 설정보다 우선 적용됩니다. 계정은 적용 또는 상위 노드로부터의 상속을 통해 구성 정책에 연결될 수 있습니다. 적용된 대상의 하위 계정 및 OU는 특별히 제외되거나, 자체 관리되거나, 다른 구성 정책을 사용하지 않는 한 이 구성 정책을 자동으로 상속합니다.

Security Hub CSPM API

구성 정책을 만들고 연결하려면

1. 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 CreateConfigurationPolicy API를 간접적으로 호출합니다.
2. `Name`에서 구성 정책의 고유한 이름을 입력합니다. 필요에 따라 `Description`에서 구성 정책에 대한 설명을 제공할 수 있습니다.
3. `ServiceEnabled` 필드에서는 이 구성 정책에서 Security Hub CSPM을 활성화 또는 비활성화할지 여부를 지정합니다.
4. `EnabledStandardIdentifiers` 필드에서는 이 구성 정책에서 활성화할 Security Hub CSPM 표준을 지정합니다.
5. `SecurityControlsConfiguration` 개체에서는 이 구성 정책에서 활성화 또는 비활성화하려는 제어를 지정합니다. `EnabledSecurityControlIdentifiers`을(를) 선택하면 지정된 제어가 활성화됩니다. 활성화된 표준에 속하는 다른 제어(새롭게 릴리스된 제어 포함)는 비활성화됩니다. `DisabledSecurityControlIdentifiers`을(를) 선택하면 지정된 제어가 비활성화됩니다. 활성화된 표준에 속하는 다른 제어(새롭게 릴리스된 제어 포함)는 활성화됩니다.
6. 필요에 따라 파라미터를 사용자 지정하려는 활성화된 제어를 `SecurityControlCustomParameters` 필드에 지정할 수 있습니다. `ValueType` 필드에 `CUSTOM`을(를) 입력하고 `Value` 필드에 사용자 지정 파라미터 값을 입력합니다. 값은 올바른 데이터 유형이어야 하며 Security Hub CSPM에서 지정한 유효한 범위 내에 있어야 합니다. 일부 제어만 사용자 지정 파라미터 값을 지원합니다. 자세한 내용은 Security Hub CSPM의 제어 파라미터 이해 단원을 참조하십시오.
7. 구성 정책을 계정 또는 OU에 적용하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 StartConfigurationPolicyAssociation API를 간접적으로 호출합니다.
8. `ConfigurationPolicyIdentifier` 필드에는 정책의 Amazon 리소스 이름(ARN) 범용 고유 식별자(UUID)를 입력합니다. 이 ARN과 UUID는 `CreateConfigurationPolicy` API에 의해 반환됩니다. 자체 관리형 구성의 경우, `ConfigurationPolicyIdentifier` 필드는 `SELF_MANAGED_SECURITY_HUB`와(과) 같습니다.
9. `Target` 필드에는 이 구성 정책을 적용할 OU, 계정 또는 루트 ID를 입력합니다. API 요청별로 하나의 대상만 입력할 수 있습니다. 선택한 대상의 하위 계정 및 OU는 자체 관리형이거나 다른 구성 정책을 사용하지 않는 한 이 구성 정책을 자동으로 상속합니다.

구성 정책을 생성하기 위한 API 요청 예제:

```
{
    "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
                                }
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

구성 정책을 연결하기 위한 API 요청 예제:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}
```

AWS CLI

구성 정책을 만들고 연결하려면

1. 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 create-configuration-policy 명령을 실행합니다.
2. name에서 구성 정책의 고유한 이름을 입력합니다. 필요에 따라 description에서 구성 정책에 대한 설명을 제공할 수 있습니다.
3. ServiceEnabled 필드에서는 이 구성 정책에서 Security Hub CSPM을 활성화 또는 비활성화할지 여부를 지정합니다.
4. EnabledStandardIdentifiers 필드에서는 이 구성 정책에서 활성화할 Security Hub CSPM 표준을 지정합니다.
5. SecurityControlsConfiguration 필드에서는 이 구성 정책에서 활성화 또는 비활성화하려는 제어를 지정합니다. EnabledSecurityControlIdentifiers을(를) 선택하면 지정된 제어가 활성화됩니다. 활성화된 표준에 속하는 다른 제어(새롭게 릴리스된 제어 포함)는 비활성화됩니다. DisabledSecurityControlIdentifiers을(를) 선택하면 지정된 제어가 비활성화됩니다. 활성화된 표준에 적용되는 다른 제어(새롭게 릴리스된 제어 포함)는 활성화됩니다.
6. 필요에 따라 파라미터를 사용자 지정하려는 활성화된 제어를 SecurityControlCustomParameters 필드에 지정할 수 있습니다. ValueType 필드에 CUSTOM을(를) 입력하고 Value 필드에 사용자 지정 파라미터 값을 입력합니다. 값은 올바른 데이터 유형이어야 하며 Security Hub CSPM에서 지정한 유효한 범위 내에 있어야 합니다. 일부 제어만 사용자 지정 파라미터 값을 지원합니다. 자세한 내용은 Security Hub CSPM의 제어 파라미터 이해 단원을 참조하십시오.
7. 구성 정책을 계정 또는 OU에 적용하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 start-configuration-policy-association 명령을 실행합니다.
8. configuration-policy-identifier 필드에는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. 이 ARN과 ID는 create-configuration-policy 명령에 의해 반환됩니다.
9. target 필드에는 이 구성 정책을 적용할 OU, 계정 또는 루트 ID를 입력합니다. 명령을 실행할 때마다 하나의 대상만 입력할 수 있습니다. 선택한 대상의 하위 항목은 자체 관리형이거나 다른 구성 정책을 사용하지 않는 한 이 구성 정책을 자동으로 상속합니다.

구성 정책을 만들기 위한 명령 예제:

```
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}}}}]}}'
```

구성 정책을 연결하기 위한 명령 예제:

```
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` API는 `AssociationStatus`(이)라는 필드를 반환합니다. 이 필드는 정책 연결이 보류 중인지 또는 성공 또는 실패 상태인지를 알려줍니다. `PENDING`에서 `SUCCESS` 또는 `FAILURE`(으)로 상태가 변경되려면 최대 24시간이 걸릴 수 있습니다. 연결 상태에 대한 자세한 내용은 구성 정책의 연결 상태 검토 섹션을 참조하세요.

## 구성 정책의 상태 및 세부 정보 검토

위임된 AWSSecurity Hub CSPM 관리자는 조직의 구성 정책과 세부 정보를 볼 수 있습니다. 여기에는 정책이 연결된 계정 및 조직 단위(OU)가 포함됩니다.

중앙 구성의 이점과 작동 방식에 대한 배경 정보는 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

원하는 방법을 선택하고 다음 단계에 따라 정책 구성을 확인하세요.

Security Hub CSPM console

구성 정책(콘솔)을 보려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택하여 구성 정책의 개요를 확인합니다.
4. 구성 정책과 세부 정보 보기를 차례로 선택하여 어느 계정 및 OU가 연결되었는지를 포함한 추가 세부 정보를 확인합니다.

Security Hub CSPM API

모든 구성 정책의 요약 목록을 보려면 Security Hub CSPM API의 ListConfigurationPolicies 작업을 사용합니다. 를 사용하는 경우 list-configuration-policies 명령을 AWS CLI실행합니다. 위임된 Security Hub CSPM 관리자 계정은 홈 리전의 작업을 간접적으로 호출합니다.

```
$ aws securityhub list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqSOhvw3o2JqjI23QDxdf
```

특정 구성 정책에 대한 세부 정보를 보려면 GetConfigurationPolicy 작업을 사용합니다. 를 사용하는 경우를 AWS CLI실행합니다get-configuration-policy. 위임된 관리자 계정은 홈 리전의 작업을 호출합니다. 세부 정보를 확인할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.

```
$ aws securityhub get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

모든 구성 정책 및 해당 계정 연결의 요약 목록을 보려면 ListConfigurationPolicyAssociations 작업을 사용합니다. 를 사용하는 경우 list-configuration-policy-associations 명령을 AWS CLI실행합니다. 위임된 관리자 계정은 홈 리전의 작업을 호출합니다. 필요에 따라 페이지 매김 파라미터를 제공하거나 특정 정책 ID, 연결 유형 또는 연결 상태를 기준으로 결과를 필터링할 수 있습니다.

```
$ aws securityhub list-configuration-policy-associations \
--filters '{"AssociationType": "APPLIED"}'
```

특정 계정에 대한 연결을 보려면 GetConfigurationPolicyAssociation 작업을 사용합니다. 를 사용하는 경우 get-configuration-policy-association 명령을 AWS CLI실행합니다. 위임된 관리자 계정은 홈 리전의 작업을 호출합니다. target에서 계정 번호, OU ID 또는 루트 ID를 입력합니다.

```
$ aws securityhub get-configuration-policy-association \
--target '{"AccountId": "123456789012"}'
```

구성 정책의 연결 상태 검토

다음 중앙 구성 API 작업은 AssociationStatus 필드를 반환합니다.

- BatchGetConfigurationPolicyAssociations
- GetConfigurationPolicyAssociation
- ListConfigurationPolicyAssociations
- StartConfigurationPolicyAssociation

이 필드는 기본 구성이 구성 정책인 경우와 자체 관리형 동작인 경우, 모두 반환됩니다.

AssociationStatus의 값은 특정 계정에 대한 정책 연결이 보류 중인지 또는 성공 또는 실패 상태인지를 알려줍니다. PENDING에서 SUCCESS 또는 FAILED(으)로 상태가 변경되려면 최대 24시간이 걸릴 수 있습니다. SUCCESS 상태는 구성 정책에 지정된 모든 설정이 계정과 연결되어 있음을 의미합니다. FAILED 상태는 구성 정책에 지정된 하나 이상의 설정이 계정과 연결되지 않았음을 의미합니다. FAILED 상태에도 불구하고 정책에 따라 계정을 부분적으로 구성할 수 있습니다. 예를 들어 Security Hub CSPM을 활성화하고AWS, 기본 보안 모범 사례를 활성화하고, CloudTrail.1. 처음 2개 설정은 성공할 수 있지만 CloudTrail.1 설정은 실패할 수 있습니다. 이 예제에서, 일부 설정이 올바르게 구성되었더라도 연결 상태는 FAILED입니다.

상위 OU 또는 루트의 연결 상태는 해당 하위 항목의 상태에 따라 달라집니다. 모든 하위 항목의 연결 상태가 SUCCESS인 경우, 상위 항목의 연결 상태는 SUCCESS입니다. 하위 항목 하나 이상의 연결 상태가 FAILED인 경우 상위 항목의 연결 상태는 FAILED입니다.

AssociationStatus의 값은 모든 관련 리전에서 정책의 연결 상태에 따라 달라집니다. 홈 리전 및 연결된 모든 리전에서 연결이 성공하면 AssociationStatus의 값은 SUCCESS입니다. 이러한 리전 중 하나 이상에서 연결이 실패할 경우, AssociationStatus의 값은 FAILED입니다.

다음과 같은 동작은 AssociationStatus의 값에도 영향을 미칩니다.

- 대상이 상위 OU이거나 루트인 경우, 모든 하위 항목이 SUCCESS 또는 FAILED 상태일 때만 AssociationStatus이 SUCCESS 또는 FAILED입니다. 상위 항목을 구성에 처음 연결한 후 하위 계정 또는 OU의 연결 상태가 변경되는 경우(예: 연결된 리전이 추가 또는 제거되는 경우), StartConfigurationPolicyAssociation API를 다시 호출하지 않는 한 상위 항목의 연결 상태가 업데이트되지 않습니다.
- 대상이 계정이면, 홈 리전 및 연결된 모든 리전에서 연결 결과가 SUCCESS 또는 FAILED인 경우에만 AssociationStatus이 SUCCESS 또는 FAILED입니다. 대상 계정을 구성과 처음 연결한 후 대상 계정의 연결 상태가 변경되면(예: 연결된 리전이 추가 또는 제거되는 경우), 해당 연결 상태가 업데이트됩니다. 하지만 StartConfigurationPolicyAssociation API를 다시 호출하지 않는 한 변경으로 인해 상위 항목의 연결 상태가 업데이트되지 않습니다.

연결된 새로운 리전을 추가하는 경우, Security Hub CSPM은 새로운 리전의 PENDING, SUCCESS 또는 FAILED 상태에 있는 기존 연결을 복제합니다.

연결 상태가 SUCCESS인 경우에도 정책의 일부인 표준의 활성화 상태는 불완전 상태로 전환될 수 있습니다. 이 경우 Security Hub CSPM은 표준의 제어에 대한 조사 결과를 생성할 수 없습니다. 자세한 내용은 표준의 상태 확인 단원을 참조하십시오.

연결 실패 문제 해결

AWSSecurity Hub CSPM에서는 다음과 같은 일반적인 이유로 구성 정책 연결이 실패할 수 있습니다.

- Organizations 관리 계정이 멤버가 아님 - 구성 정책을 Organizations 관리 계정과 연결하려면 해당 계정에 이미 AWSSecurity Hub CSPM이 활성화되어 있어야 합니다. 여기에는 관리 계정과 조직의 모든 구성원 계정이 포함됩니다.
- AWS Config가 활성화되지 않았거나 올바르게 구성되지 않음 - 구성 정책에서 표준을 활성화하려면 관련 리소스를 기록하도록 활성화하고 구성해야 AWS Config합니다.
- 위임된 관리자 계정에서 연결해야 함 - 위임된 Security Hub CSPM 관리자 계정에 로그인한 경우에만 대상 계정 및 OU에 정책을 연결할 수 있습니다.
- 홈 리전에서 연결해야 함 - 홈 리전에 로그인한 경우에만 대상 계정 및 OU에 정책을 연결할 수 있습니다.
- 옵트인 영역이 활성화되지 않음 – 위임된 관리자가 활성화하지 않은 옵트인 리전인 경우, 연결된 리전의 구성원 계정 또는 OU에 대한 정책 연결이 실패합니다. 위임된 관리자 계정에서 리전을 활성화한 후 다시 시도할 수 있습니다.
- 구성원 계정 일시 중단됨 – 정책을 일시 중지된 구성원 계정과 연결하려고 하면 정책 연결이 실패합니다.

## 구성 정책 업데이트

구성 정책을 생성한 후 위임된 AWS Security Hub CSPM 관리자 계정은 정책 세부 정보 및 정책 연결을 업데이트할 수 있습니다. 정책 세부 정보가 업데이트되면 구성 정책에 연결된 계정이 업데이트된 정책을 자동으로 사용하기 시작합니다.

중앙 구성의 이점과 작동 방식에 대한 배경 정보는 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

> **Note**
>
> 구성 정책은 AWS 표준 및 제어만 지원합니다. 구성 정책에 멀티클라우드 표준(예: CIS Azure Foundations Benchmark v4.0.0) 또는 Azure 제어를 포함할 수 없습니다. 멀티클라우드 표준 ARN 또는 제어 ID를 포함하면가 반환됩니다`InvalidInputException`. 멀티클라우드 표준을 활성화하거나 구성하려면 원하는에서 직접 로컬 구성 메커니즘을 사용합니다 AWS 계정.

위임된 관리자는 다음 정책 설정을 업데이트할 수 있습니다.

- Security Hub CSPM을 활성화하거나 비활성화합니다.
- 하나 이상의 보안 표준을 활성화합니다.
- 활성화된 표준 전반에서 어떤 보안 제어를 사용할 수 있는지 표시합니다. 이를 위해 활성화해야 하는 특정 제어 목록을 제공할 수 있습니다. 그러면 Security Hub CSPM은 새로운 제어가 릴리스될 때 새로운 제어를 포함한 다른 모든 제어를 비활성화합니다. 또는 비활성화해야 하는 특정 제어의 목록을 제공할 수 있습니다. 그러면 Security Hub CSPM은 새로운 제어가 릴리스될 때 새로운 제어를 포함한 다른 모든 제어를 활성화합니다.
- 사용 가능한 표준에서 사용할 수 있는 제어를 선택할 수 있도록 파라미터를 사용자 지정할 수도 있습니다.

원하는 방법을 선택하고 다음 단계에 따라 구성 정책을 업데이트하세요.

> **Note**
>
> 중앙 구성을 사용하는 경우, Security Hub CSPM은 홈 리전을 제외한 모든 리전의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 활성화하도록 선택한 다른 제어는 사용 가능한 모든 리전에서 활성화됩니다. 이러한 컨트롤에 대한 결과를 한 리전으로만 제한하려면 AWS Config 레코더 설정을 업데이트하고 홈 리전을 제외한 모든 리전에서 글로벌 리소스 기록을 끌 수 있습니다.

글로벌 리소스를 평가하는 활성화된 제어가 홈 리전에서 지원되지 않는 경우 Security Hub CSPM은 해당 제어가 지원되는 연결된 리전에서 제어를 활성화하려고 시도합니다. 중앙 구성을 사용하는 경우, 홈 리전 또는 연결된 리전에서 사용할 수 없는 제어에 대한 적용 범위가 부족합니다.
글로벌 리소스와 관련된 제어 목록은 글로벌 리소스를 사용하는 제어 섹션을 참조하세요.

Console

구성 정책을 업데이트하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다.
4. 편집할 구성 정책을 선택하고 편집을 선택합니다. 원하는 경우, 정책 설정을 편집합니다. 정책 설정을 변경하지 않으려면 이 섹션을 그대로 둡니다.
5. 다음을 선택합니다. 원하는 경우, 정책 연결을 편집합니다. 정책 연결을 변경하지 않으려면 이 섹션을 그대로 둡니다. 정책을 업데이트할 때, 최대 15개의 대상(계정, OU 또는 루트)과 연결하거나 연결 해제할 수 있습니다.
6. 다음을 선택합니다.
7. 변경 사항을 검토하고 저장 및 적용을 선택합니다. 홈 리전 및 연결된 리전에서 이 작업은 이 구성 정책과 연결된 계정의 기존 구성 설정보다 우선 적용됩니다. 계정은 적용 또는 상위 노드로부터의 상속을 통해 구성 정책에 연결될 수 있습니다.

API

구성 정책을 업데이트하려면

1. 구성 정책의 설정을 업데이트하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 UpdateConfigurationPolicy API를 간접적으로 호출합니다.
2. 업데이트할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `ConfigurationPolicy` 아래 필드에 업데이트된 값을 입력합니다. 필요에 따라 업데이트 이유를 입력할 수도 있습니다.

4. 이 구성 정책에 새로운 연결을 추가하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 StartConfigurationPolicyAssociation API를 간접적으로 호출합니다. 현재 연결을 하나 이상 제거하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 StartConfigurationPolicyDisassociation API를 간접적으로 호출합니다.
5. `ConfigurationPolicyIdentifier` 필드에는 연결을 업데이트하려는 구성 정책의 ARN 또는 ID를 입력합니다.
6. `Target` 필드에 연결하거나 연결 해제하려는 계정, OU 또는 루트 ID를 입력합니다. 이 작업은 지정된 OU 또는 계정에 대한 이전 정책 연결을 무시합니다.

> **Note**
>
> `UpdateConfigurationPolicy` API를 간접적으로 호출하면 Security Hub CSPM 은 `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` 및 `SecurityControlCustomParameters` 필드의 전체 목록 대체를 수행합니다. 이 API를 호출할 때마다 활성화하려는 표준의 전체 목록과 활성화 또는 비활성화하고 파라미터를 사용자 지정하려는 제어의 전체 목록을 제공하세요.

구성 정책을 업데이트하기 위한 API 요청 예제:

```
{
    "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

구성 정책을 업데이트하려면

1. 구성 정책의 설정을 업데이트하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 update-configuration-policy 명령을 실행합니다.
2. 업데이트할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `configuration-policy` 아래 필드에 업데이트된 값을 입력합니다. 필요에 따라 업데이트 이유를 입력할 수도 있습니다.
4. 이 구성 정책에 새로운 연결을 추가하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 start-configuration-policy-association 명령을 실행합니다. 현재 연결을 하나 이상 제거하려면 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 start-configuration-policy-disassociation 명령을 실행합니다.
5. `configuration-policy-identifier` 필드에는 연결을 업데이트하려는 구성 정책의 ARN 또는 ID를 입력합니다.
6. `target` 필드에 연결하거나 연결 해제하려는 계정, OU 또는 루트 ID를 입력합니다. 이 작업은 지정된 OU 또는 계정에 대한 이전 정책 연결을 무시합니다.

> **Note**
>
> `update-configuration-policy` 명령을 실행하면 Security Hub CSPM은 `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` 및 `SecurityControlCustomParameters` 필드의 전체 목록 대체를 수행합니다. 이 명령을 실행할 때마다 활성화하려는 표준의 전체 목록과 활성화 또는 비활성화하고 파라미터를 사용자 지정하려는 제어의 전체 목록을 제공하세요.

구성 정책을 업데이트하기 위한 명령 예제:

```
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` API는 `AssociationStatus`(이)라는 필드를 반환합니다. 이 필드는 정책 연결이 보류 중인지 또는 성공 또는 실패 상태인지를 알려줍니다. `PENDING`에서 `SUCCESS` 또는 `FAILURE`(으)로 상태가 변경되려면 최대 24시간이 걸릴 수 있습니다. 연결 상태에 대한 자세한 내용은 구성 정책의 연결 상태 검토 섹션을 참조하세요.

## 구성 정책 삭제

구성 정책을 생성한 후 위임된 AWSSecurity Hub CSPM 관리자는 이를 삭제할 수 있습니다. 또는 위임된 관리자가 구성 정책을 유지하되 특정 계정이나 OU(조직 단위) 또는 루트와의 연결을 해제할 수도 있습니다. 정책 연결 해제에 대한 지침은 대상에서 구성 연결 해제 섹션을 참조하세요.

중앙 구성의 이점과 작동 방식에 대한 배경 정보는 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

이 섹션에서는 구성 정책을 삭제하는 방법을 설명합니다.

구성 정책을 삭제하면 해당 구성 정책은 조직에 더 이상 존재하지 않습니다. 대상 계정, OU 및 조직 루트는 더 이상 구성 정책을 사용할 수 없습니다. 삭제된 구성 정책과 연결된 대상은 가장 가까운 상위 항목의 구성 정책을 상속하거나 가장 가까운 상위 그룹이 자체 관리형인 경우, 자체 관리형이 됩니다. 대상이 다른 구성을 사용하도록 하려면 대상을 새로운 구성 정책에 연결하세요. 자세한 내용은 구성 정책 생성 및 연결 섹션을 참조하세요.

적절한 보안 범위를 제공하려면 구성 정책을 하나 이상 만들어 조직에 연결하는 것이 좋습니다.

구성 정책을 삭제하려면 먼저 해당 정책이 현재 적용되는 계정, OU 또는 루트에서 정책을 연결 해제해야 합니다.

원하는 방법을 선택하고 다음 단계에 따라 구성 정책을 삭제하세요.

Console

구성 정책을 삭제하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다. 삭제하려는 구성 정책을 선택한 다음 삭제를 선택합니다. 구성 정책이 여전히 계정이나 OU와 연결되어 있는 경우, 정책을 삭제하기 전에 먼저 해당 대상에서 정책을 연결 해제하라는 메시지가 표시됩니다.
4. 확인 메시지를 검토합니다. **`confirm`**을(를) 입력한 다음 삭제를 선택합니다.

API

구성 정책을 삭제하려면

홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 DeleteConfigurationPolicy API를 간접적으로 호출합니다.

삭제할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. `ConflictException` 오류가 발생하더라도 구성 정책은 조직의 계정 또는 OU에 계속 적용됩니다. 오류를 해결하려면 구성 정책을 삭제하기 전에 이러한 계정이나 OU에서 구성 정책을 연결 해제하세요.

구성 정책을 삭제하기 위한 API 요청 예제:

```
{
    "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

구성 정책을 삭제하려면

홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 delete-configuration-policy 명령을 실행합니다.

삭제할 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. `ConflictException` 오류가 발생하더라도 구성 정책은 조직의 계정 또는 OU에 계속 적용됩니다. 오류를 해결하려면 구성 정책을 삭제하기 전에 이러한 계정이나 OU에서 구성 정책을 연결 해제하세요.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

## 대상에서 구성 연결 해제

위임된 AWSSecurity Hub CSPM 관리자 계정에서 구성 정책 또는 자체 관리형 구성을 계정, OU 또는 루트에서 연결 해제할 수 있습니다. 연결 해제는 나중에 사용할 수 있도록 정책을 유지하지만 특정 계정, OU 또는 루트에서 기존 연결을 제거합니다. 상속된 구성이 아닌 직접 적용된 구성만 연결 해제할 수 있습니다. 상속된 구성을 변경하려면 영향을 받는 계정 또는 OU에 구성 정책 또는 자체 관리형 동작을 적용할 수 있습니다. 원하는 수정 사항이 포함된 새로운 구성 정책을 가장 가까운 상위 항목에 적용할 수도 있습니다.

연결을 해제해도 구성 정책은 삭제되지 않습니다. 정책은 계정에 유지되므로 조직의 다른 대상과 연결할 수 있습니다. 구성 정책 삭제에 대한 지침은 구성 정책 삭제 섹션을 참조하세요. 연결 해제가 완료되면 영향을 받는 대상은 가장 가까운 상위 항목의 구성 정책 또는 자체 관리형 동작을 상속합니다. 상속 가능한 구성이 없는 경우, 대상은 연결 해제 이전의 설정을 유지하지만 자체 관리형이 됩니다.

원하는 방법을 선택하고 단계에 따라 계정, OU 또는 루트를 현재 구성에서 연결 해제하세요.

Console

현재 구성에서 계정 또는 OU의 연결을 해제하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. Organizations 탭에서 현재 구성과 연결 해제하려는 계정, OU 또는 루트를 선택합니다. 편집을 선택합니다.
4. 위임된 관리자가 대상에 직접 정책을 적용할 수 있도록 하려면 구성 정의 페이지의 관리에서 정책 적용을 선택합니다. 대상이 가장 가까운 상위 항목의 구성을 상속하도록 하려면 상속을 선택합니다. 두 경우 모두 위임된 관리자가 대상의 설정을 제어합니다. 계정이나 OU에서 자체 설정을 제어하도록 하려면 자체 관리형을 선택합니다.
5. 변경 사항을 검토한 후 다음을 선택하고 적용을 선택합니다. 이 작업은 범위 내에 있는 계정 또는 OU의 기존 구성이 현재 선택 항목과 충돌하는 경우, 해당 구성을 무시합니다.

API

현재 구성에서 계정 또는 OU의 연결을 해제하려면

1. 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 StartConfigurationPolicyDisassociation API를 간접적으로 호출합니다.
2. `ConfigurationPolicyIdentifier`에는 연결을 해제하려는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. 자체 관리형 동작을 분리하려면 이 필드에 `SELF_MANAGED_SECURITY_HUB`을(를) 입력합니다.
3. `Target`에서는 이 구성 정책에서 연결 해제하려는 계정, OU 또는 루트를 입력합니다.

구성 정책의 연결을 해제하기 위한 API 요청 예제:

```
{
    "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

현재 구성에서 계정 또는 OU의 연결을 해제하려면

1. 홈 리전의 Security Hub CSPM 위임된 관리자 계정에서 start-configuration-policy-disassociation 명령을 실행합니다.
2. `configuration-policy-identifier`에는 연결을 해제하려는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다. 자체 관리형 동작을 분리하려면 이 필드에 `SELF_MANAGED_SECURITY_HUB`을(를) 입력합니다.
3. `target`에서는 이 구성 정책에서 연결 해제하려는 계정, OU 또는 루트를 입력합니다.

구성 정책의 연결을 해제하기 위한 명령 예제:

```
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"}'
```

## 컨텍스트별로 표준 또는 제어 구성

AWSSecurity Hub CSPM에서 중앙 구성을 사용하는 경우 위임된 Security Hub CSPM 관리자는 조직에 대해 Security Hub CSPM, 보안 표준 및 보안 제어를 구성하는 방법을 지정하는 구성 정책을 생성할 수 있습니다. 위임된 관리자는 이 정책을 특정 계정 및 조직 단위(OU)와 연결할 수 있습니다. 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 위임된 관리자는 필요에 따라 구성 정책을 업데이트할 수 있습니다.

Security Hub CSPM 콘솔에서 위임된 관리자는 두 가지 방법으로, 즉 구성 페이지에서 또는 기존 워크플로의 컨텍스트별로 구성 정책을 업데이트할 수 있습니다. 보안 조사 결과를 검토하면서 환경에 가장 적합한 표준 및 제어를 발견하고 동시에 구성할 수 있기 때문에 후자가 더 유용할 수 있습니다.

컨텍스트별 구성은 Security Hub CSPM 콘솔에서만 사용할 수 있습니다. 위임된 관리자는 Security Hub CSPM API의 UpdateConfigurationPolicy 작업을 간접적으로 호출하여 조직에서 특정 표준 또는 제어가 구성되는 방식을 프로그래밍 방식으로 변경해야 합니다.

다음 단계에 따라 컨텍스트별로 Security Hub CSPM 표준 또는 제어를 구성합니다.

컨텍스트별로 표준 또는 제어를 구성하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 왼쪽 탐색 창에서 다음 옵션 중 하나를 선택합니다.

   - 표준을 구성하려면 보안 표준을 선택하고 특정 표준을 선택합니다.
   - 제어를 구성하려면 제어를 선택하고 특정 제어를 선택합니다.
3. 콘솔에는 기존 Security Hub CSPM 구성 정책과 각 정책에서 선택된 표준 또는 제어의 상태가 나열됩니다. 각 구성 정책에서 옵션을 선택하여 표준 또는 제어를 활성화하거나 비활성화합니다. 제어의 경우, 제어 파라미터를 사용자 지정하도록 선택할 수도 있습니다. 컨텍스트 내 구성 중에는 새로운 정책을 생성할 수 없습니다. 새로운 정책을 생성하려면 구성 페이지로 이동하여 정책 탭을 선택한 다음 정책 생성을 선택해야 합니다.
4. 변경한 후 다음을 선택합니다.
5. 변경 사항을 검토하고 적용을 선택합니다. 업데이트는 변경된 구성 정책과 연결된 모든 계정 및 OU에 영향을 미칩니다. 업데이트는 홈 리전 및 연결된 모든 리전에도 적용됩니다.

## Security Hub CSPM의 중앙 구성 비활성화

AWSSecurity Hub CSPM에서 중앙 구성을 비활성화하면 위임된 관리자는 여러 AWS 계정조직 단위(OUs) 및에서 Security Hub CSPM, 보안 표준 및 보안 제어를 구성할 수 없습니다AWS 리전. 대신 각 리전의 각 계정에 대해 대부분의 설정을 개별적으로 구성해야 합니다.

> **Important**
>
> 중앙 구성을 비활성화하기 전에 먼저, 구성 정책이든 자체 관리형 동작이든 관계없이 현재 구성에서 계정과 OU의 연결을 해제해야 합니다.
> 중앙 구성 사용을 비활성화하기 전에 먼저 기존 구성 정책도 삭제해야 합니다.

중앙 구성을 비활성화하면 다음과 같은 변경 사항이 발생합니다.

- 위임된 관리자는 더 이상 조직에 대한 구성 정책을 만들 수 없습니다.
- 구성 정책이 적용되거나 상속된 계정은 현재 설정이 유지되지만 자체 관리형이 됩니다.
- 조직이 로컬 구성으로 전환합니다. 로컬 구성에서는 대부분의 Security Hub CSPM 설정을 각 조직 계정 및 리전에서 개별적으로 구성해야 합니다. 위임된 관리자는 Security Hub CSPM, 기본 보

안 표준 및 새로운 조직 계정의 기본 표준에 속하는 모든 제어를 자동으로 활성화하도록 선택할 수 있습니다. 기본 표준은 AWSFoundational Security Best Practices(FSBP) 및 Center for Internet Security(CIS)AWSFoundations Benchmark v1.2.0입니다. 이러한 설정은 현재 리전에만 적용되며 새로운 조직 계정에만 영향을 미칩니다. 위임된 관리자는 기본값인 표준을 변경할 수 없습니다. 로컬 구성에서는 구성 정책 또는 OU 수준의 구성 사용을 지원하지 않습니다.

중앙 구성 사용을 중지해도 위임된 관리자 계정의 ID는 동일하게 유지됩니다. 홈 리전과 연결된 리전도 동일하게 유지됩니다(홈 리전은 이제 집계 영역이라고 하며 결과 집계에 사용할 수 있음).

원하는 방법을 선택하고 단계에 따라 중앙 구성 사용을 중단하고 로컬 구성으로 전환하세요.

Security Hub CSPM console

중앙 구성을 비활성화하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 개요 섹션에서 편집을 선택합니다.
4. 조직 구성 편집 상자에서 로컬 구성을 선택합니다. 아직 연결을 해제하지 않은 경우, 중앙 구성을 중지하려면 먼저 현재 구성 정책을 연결 해제하고 삭제하라는 메시지가 표시됩니다. 자체 관리형으로 지정된 계정 또는 OU는 자체 관리형 구성과의 연결을 해제해야 합니다. 콘솔에서 각 자체 관리형 계정 또는 OU의 관리 유형을 중앙 관리형 및 나의 조직에서 상속으로 변경하여 이 작업을 수행할 수 있습니다.
5. 필요에 따라 새로운 조직 계정의 로컬 구성 기본 설정을 선택합니다.
6. 확인을 선택합니다.

Security Hub CSPM API

중앙 구성(API)을 비활성화하려면

1. UpdateOrganizationConfiguration API를 호출합니다.
2. `OrganizationConfiguration` 객체의 `ConfigurationType` 필드를 `LOCAL`(으)로 설정합니다. 기존 구성 정책 또는 정책 연결이 있는 경우, API는 오류를 반환합니다. 구성 정책을 연결 해제하려면 `StartConfigurationPolicyDisassociation` API를 호출합니다. 구성 정책을 삭제하려면 `DeleteConfigurationPolicy` API를 호출합니다.

3. 새로운 조직 계정에서 Security Hub CSPM을 자동으로 활성화하려면 `AutoEnable` 필드를 `true`로 설정합니다. 기본적으로 이 필드의 값은 `false`이며 Security Hub CSPM은 새로운 조직 계정에서 자동으로 활성화되지 않습니다. 필요에 따라 새로운 조직 계정에서 기본 보안 표준을 자동으로 활성화하려면 `AutoEnableStandards` 필드를 `DEFAULT`(으)로 설정합니다. 이것이 기본값입니다. 새로운 조직 계정에서 기본 보안 표준을 자동으로 활성화하지 않으려면 `AutoEnableStandards` 필드를 `NONE`(으)로 설정합니다.

API 요청 예제:

```
{
    "AutoEnable": true,
    "OrganizationConfiguration": {
        "ConfigurationType" : "LOCAL"
    }
}
```

AWS CLI

중앙 구성을 비활성화하려면(AWS CLI)

1. update-organization-configuration 명령을 실행합니다.
2. `organization-configuration` 객체의 `ConfigurationType` 필드를 `LOCAL`(으)로 설정합니다. 기존 구성 정책 또는 정책 연결이 있는 경우, 이 명령은 오류를 반환합니다. 구성 정책을 연결 해제하려면 `start-configuration-policy-disassociation` 명령을 실행합니다. 구성 정책을 삭제하려면 `delete-configuration-policy` 명령을 실행합니다.
3. 새로운 조직 계정에서 Security Hub CSPM을 자동으로 활성화하려면 `auto-enable` 파라미터를 포함합니다. 기본적으로 이 파라미터의 값은 `no-auto-enable`이며 Security Hub CSPM은 새로운 조직 계정에서 자동으로 활성화되지 않습니다. 필요에 따라 새로운 조직 계정에서 기본 보안 표준을 자동으로 활성화하려면 `auto-enable-standards` 필드를 `DEFAULT`(으)로 설정합니다. 이것이 기본값입니다. 새로운 조직 계정에서 기본 보안 표준을 자동으로 활성화하지 않으려면 `auto-enable-standards` 필드를 `NONE`(으)로 설정합니다.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

# Security Hub CSPM의 관리자 및 멤버 계정 관리

AWS환경에 여러 계정이 있는 경우 AWSSecurity Hub CSPM을 멤버 계정으로 사용하는 계정을 취급하고 단일 관리자 계정과 연결할 수 있습니다. 관리자는 전반적인 보안 태세를 모니터링하고 멤버 계정에 대해 허용된 작업을 수행할 수 있습니다. 또한 관리자는 예상 사용 비용 모니터링 및 계정 할당량 평가와 같은 다양한 계정 관리 및 관리 작업을 대규모로 수행할 수 있습니다.

Security Hub CSPM을와 통합AWS Organizations하거나 Security Hub CSPM에서 멤버십 초대를 수동으로 보내고 수락하여 두 가지 방법으로 멤버 계정을 관리자와 연결할 수 있습니다.

## 를 사용하여 계정 관리AWS Organizations

AWS Organizations는 AWS관리자가 여러를 통합하고 관리할 수 있는 글로벌 계정 관리 서비스입니다 AWS 계정. 예산, 보안 및 규정 준수 요구 사항을 지원하도록 설계된 계정 관리 및 통합 결제 기능을 제공합니다. 추가 비용 없이 제공되며 AWSSecurity Hub CSPM, Amazon Macie 및 Amazon GuardDuty를 AWS 서비스비롯한 여러와 통합됩니다. 자세한 내용은 AWS Organizations 사용 설명서를 참조하십시오.

Security Hub CSPM과 AWS Organizations를 통합하면 Organizations 관리 계정이 Security Hub CSPM 위임된 관리자를 지정합니다. Security Hub CSPM은 AWS 리전지정된의 위임된 관리자 계정에서 자동으로 활성화됩니다.

위임된 관리자를 지정한 후에는 중앙 구성을 사용하여 Security Hub CSPM에서 계정을 관리하는 것이 좋습니다. 이는 Security Hub CSPM을 사용자 지정하고 조직에 적절한 보안 범위를 보장하는 가장 효율적인 방법입니다.

중앙 구성을 사용하면 위임된 관리자가 리전별로 구성하는 대신 여러 조직 계정 및 리전에서 Security Hub CSPM을 사용자 지정할 수 있습니다. 전체 조직에 대한 구성 정책을 만들거나 계정 및 OU별로 다른 구성 정책을 만들 수 있습니다. 정책은 관련 계정에서 Security Hub CSPM을 활성화 또는 비활성화할지 여부와 활성화되는 보안 표준 및 제어를 지정합니다.

위임된 관리자는 계정을 중앙 관리형 계정 또는 자체 관리형 계정으로 지정할 수 있습니다. 중앙 관리형 계정은 위임된 관리자만 구성할 수 있습니다. 자체 관리형 계정은 자체 설정을 지정할 수 있습니다.

중앙 구성을 선택하지 않으면 위임된 관리자가 Security Hub CSPM을 구성할 수 있는 권한이 더 제한되며, 이를 로컬 구성이라고 합니다. 로컬 구성에서 위임된 관리자는 현재 리전의 새로운 조직 계정에서 Security Hub CSPM 및 기본 보안 표준을 자동으로 활성화할 수 있습니다. 하지만 기존 계정에서는 이러한 설정을 사용하지 않으므로 계정이 조직에 가입한 후에 구성 드리프트가 발생할 수 있습니다.

이러한 새로운 계정 설정 외에도 로컬 구성은 계정별 및 리전별로 다릅니다. 각 조직 계정은 각 리전에서 Security Hub CSPM 서비스, 표준 및 제어를 개별적으로 구성해야 합니다. 또한 로컬 구성에서는 구성 정책 사용을 지원하지 않습니다.

## 초대를 통한 수동 계정 관리

독립형 계정이 있는 경우 또는 Organizations와 통합하지 않는 경우, Security Hub CSPM에서 초대를 통해 멤버 계정을 수동으로 관리해야 합니다. 독립형 계정은 Organizations와 통합할 수 없으므로 수동으로 관리해야 합니다. 나중에 계정을 추가하는 경우와 통합AWS Organizations하고 중앙 구성을 사용하는 것이 좋습니다.

수동 계정 관리를 사용하는 경우, 계정을 Security Hub CSPM 관리자로 지정합니다. 관리자 계정은 멤버 계정의 데이터를 보고 멤버 계정 결과에 대해 특정 작업을 수행할 수 있습니다. Security Hub CSPM 관리자는 다른 계정을 멤버 계정으로 초대하며, 예비 멤버 계정이 초대를 수락하면 관리자-멤버 관계가 성립됩니다.

수동 계정 관리는 구성 정책 사용을 지원하지 않습니다. 구성 정책이 없으면 관리자는 여러 계정에 대한 변수 설정을 구성하여 Security Hub CSPM을 중앙에서 사용자 지정할 수 없습니다. 대신 각 조직 계정은 각 리전에서 개별적으로 Security Hub CSPM을 활성화하고 구성해야 합니다. 이로 인해 Security Hub CSPM을 사용하는 모든 계정 및 리전에서 적절한 보안 범위를 보장하는 것이 더 어려워지고 시간이 많이 소요될 수 있습니다. 또한 멤버 계정이 관리자의 입력 없이 자체 설정을 지정할 수 있기 때문에 구성 드리프트가 발생할 수 있습니다.

초대를 통해 계정을 관리하려면 Security Hub CSPM에서 초대를 통한 계정 관리 섹션을 참조하세요.

## Security Hub CSPM에서 여러 계정을 관리하기 위한 권장 사항

다음 섹션에서는 AWSSecurity Hub CSPM에서 멤버 계정을 관리할 때 유의해야 할 몇 가지 제한 및 권장 사항을 요약합니다.

### 멤버 계정 최대 수

와의 통합을 사용하는 경우 AWS OrganizationsSecurity Hub CSPM은 각에서 위임된 관리자 계정당 최대 10,000개의 멤버 계정을 지원합니다AWS 리전. Security Hub CSPM을 수동으로 활성화하고 관리하는 경우, Security Hub CSPM은 각 리전에서 관리자 계정당 최대 1,000개의 멤버 계정 초대를 지원합니다.

## 관리자-회원 관계 생성

> **Note**
>
> Security Hub CSPM 통합을 사용하고 멤버 계정을 수동으로 초대하지 AWS Organizations않은 경우이 섹션은 적용되지 않습니다.

한 계정이 관리자 계정과 멤버 계정을 겸할 수 없습니다.

멤버 계정은 한 번에 하나의 관리자 계정만 연결할 수 있습니다. Security Hub CSPM 관리자 계정이 조직 계정을 활성화한 경우, 해당 계정은 다른 계정의 초대를 수락할 수 없습니다. 계정이 이미 초대를 수락한 경우, 조직의 Security Hub CSPM 관리자 계정에서 해당 계정을 활성화할 수 없습니다. 또한, 다른 계정의 초대를 받을 수 없습니다.

수동 초대 프로세스의 경우, 멤버십 초대를 수락하는 것은 선택 사항입니다.

를 통한 멤버십AWS Organizations

Security Hub CSPM을와 통합하는 경우 Organizations 관리 계정은 Security Hub CSPMAWS Organizations에 대한 위임된 관리자(DA) 계정을 지정할 수 있습니다. 조직 관리 계정은 Organizations에서 DA로 설정할 수 없습니다. Security Hub CSPM에서는 허용되지만 Organizations 관리 계정은 DA가 아닌 것이 좋습니다.

모든 리전에 DA 계정을 동일하게 선택하는 것을 권장합니다. 중앙 구성을 사용하는 경우, Security Hub CSPM은 조직의 Security Hub CSPM을 구성하는 모든 리전에서 동일한 DA 계정을 설정합니다.

또한 단일 창에서 AWS보안 관련 문제를 관리하는 데 도움이 되도록 보안 및 규정 준수 서비스 전반에서 동일한 DA 계정을 선택하는 것이 좋습니다.

초대를 통한 멤버십

초대를 통해 생성된 멤버 계정의 경우, 초대를 보낸 리전에서만 관리자-멤버 계정 연결이 생성됩니다. 관리자 계정은 Security Hub CSPM을 사용하려는 각 리전에서 Security Hub CSPM을 활성화해야 합니다. 그러면 관리자 계정이 각 계정을 해당 리전의 멤버 계정이 되도록 초대합니다.

> **Note**
>
> Security Hub CSPM 초대 AWS Organizations대신를 사용하여 멤버 계정을 관리하는 것이 좋습니다.

### 서비스 전반에서 관리자 계정 조정하기

Security Hub CSPM은 Amazon GuardDuty, Amazon Inspector, Amazon Macie와 같은 다양한 AWS서비스의 결과를 집계합니다. 또한, Security Hub CSPM을 사용하면 사용자는 GuardDuty 조사 결과에서 피벗하여 Amazon Detective에서 조사를 시작할 수 있습니다.

하지만, 이러한 다른 서비스에서 설정한 관리자-멤버 관계는 Security Hub CSPM에 자동으로 적용되지 않습니다. Security Hub CSPM은 이러한 모든 서비스에 관리자 계정과 동일한 계정을 사용할 것을 권장합니다. 이 관리자 계정은 보안 도구를 담당하는 계정이어야 합니다. 또한, 동일한 계정이 AWS Config에 대한 집계 계정이어야 합니다.

예를 들어, GuardDuty 관리자 계정 A의 사용자는 GuardDuty 콘솔에서 GuardDuty 멤버 계정 B와 C에 대한 조사 결과를 볼 수 있습니다. 그런 다음 계정 A가 Security Hub CSPM을 활성화할 경우, 계정 A의 사용자는 Security Hub CSPM에서 계정 B와 C에 대한 GuardDuty 조사 결과를 자동으로 볼 수는 없습니다. 이러한 계정에도 Security Hub CSPM 관리자-멤버 관계가 필요합니다.

이를 수행하려면, 계정 A를 Security Hub CSPM 관리자 계정으로 지정하고 계정 B와 C를 Security Hub CSPM 멤버 계정으로 활성화하세요.

## 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations

AWSSecurity Hub CSPM을와 통합AWS Organizations한 다음 조직의 계정에 대해 Security Hub CSPM을 관리할 수 있습니다.

Security Hub CSPM을와 통합하려면에서 조직을 AWS Organizations생성합니다AWS Organizations. Organizations 관리 계정은 계정 하나를 해당 조직에 대해 Security Hub CSPM 위임된 관리자로 지정합니다. 그러면 위임된 관리자는 조직의 다른 계정에 대해 Security Hub CSPM을 활성화하고, 해당 계정을 Security Hub CSPM 멤버 계정으로 추가하고, 멤버 계정에 대해 허용된 작업을 수행할 수 있습니다. Security Hub CSPM 위임된 관리자는 최대 10,000개의 멤버 계정에 대해 Security Hub CSPM을 활성화하고 관리할 수 있습니다.

위임된 관리자의 구성 기능 범위는 중앙 구성을 사용하는지 여부에 따라 달라집니다. 중앙 구성을 사용하면 각 멤버 계정 및 AWS 리전에서 개별적으로 Security Hub CSPM을 구성할 필요가 없습니다. 위임된 관리자는 여러 리전의 지정된 멤버 계정 및 조직 단위(OU)에서 특정 Security Hub CSPM 설정을 적용할 수 있습니다.

Security Hub CSPM 관리자 계정은 멤버 계정에 대해 다음 작업을 수행할 수 있습니다.

- 중앙 구성을 사용하는 경우, Security Hub CSPM 구성 정책을 생성하여 중앙에서 멤버 계정 및 OU에 대한 Security Hub CSPM을 구성합니다. 구성 정책을 사용하여 Security Hub CSPM을 활성화 및 비활성화하고, 표준을 활성화 및 비활성화하고, 제어를 활성화 및 비활성화할 수 있습니다.

- 새로운 계정이 조직에 추가될 때 자동으로 해당 계정을 Security Hub CSPM 멤버 계정으로 취급합니다. 중앙 구성을 사용하는 경우, OU와 관련된 구성 정책에는 OU에 속한 기존 계정 및 새로운 계정이 포함됩니다.
- 기존 조직 계정을 Security Hub CSPM 멤버 계정으로 취급합니다. 이는 중앙 구성을 사용하면 자동으로 이루어집니다.
- 조직에 속한 멤버 계정을 연결 해제하세요. 중앙 구성을 사용하는 경우, 멤버 계정을 자체 관리형으로 지정한 후에만 멤버 계정을 연결 해제할 수 있습니다. 또는 Security Hub CSPM을 비활성화하는 구성 정책을 특정한 중앙 관리형 멤버 계정과 연결할 수 있습니다.

중앙 구성에 옵트인하지 않으면 조직에서 로컬 구성이라는 기본 구성 유형을 사용합니다. 로컬 구성에서 위임된 관리자에게는 멤버 계정에서 설정을 적용할 수 있는 기능이 더 제한됩니다. 자세한 내용은 Security Hub CSPM의 로컬 구성 이해 섹션을 참조하세요.

위임된 관리자가 멤버 계정에 대해 수행할 수 있는 전체 작업 목록은 Security Hub CSPM에서 관리자 및 멤버 계정별로 허용된 작업 섹션을 참조하세요.

이 섹션의 주제에서는 Security Hub CSPM을 AWS Organizations와 통합하는 방법과 조직의 계정에 대해 Security Hub CSPM을 관리하는 방법을 설명합니다. 관련된 경우, 각 섹션에서는 중앙 구성 사용자를 위한 관리상의 이점과 차이점을 설명합니다.

주제

- Security Hub CSPM과 통합AWS Organizations
- 새로운 조직 계정에서 Security Hub CSPM 자동 활성화
- 새로운 조직 계정에서 Security Hub CSPM 수동 활성화
- 조직에서 Security Hub CSPM 멤버 계정 연결 해제

## Security Hub CSPM과 통합AWS Organizations

AWSSecurity Hub CSPM과를 통합하려면 Organizations에서 조직을 AWS Organizations생성하고 조직 관리 계정을 사용하여 위임된 Security Hub CSPM 관리자 계정을 지정합니다. 이렇게 하면 Security Hub CSPM이 Organizations에서 신뢰할 수 있는 서비스로 활성화됩니다. 또한 현재 AWS 리전에서 위임된 관리자 계정에 대해 Security Hub CSPM을 활성화하고, 위임된 관리자가 멤버 계정에 대해 Security Hub CSPM을 활성화하며, 멤버 계정의 데이터를 보고, 멤버 계정에서 다른 허용된 작업을 수행할 수 있습니다.

중앙 구성을 사용하는 경우, 위임된 관리자는 Security Hub CSPM 서비스, 표준 및 제어를 조직 계정에서 어떻게 구성하는지 지정하는 Security Hub CSPM 구성 정책을 만들 수도 있습니다.

조직 생성

조직은 단일 단위로 관리할 수 AWS 계정있도록를 통합하기 위해 생성하는 엔터티입니다.

AWS Organizations콘솔을 사용하거나 또는 SDK API 중 AWS CLI하나의 명령을 사용하여 조직을 생성할 수 있습니다. APIs 자세한 지침은 AWS Organizations 사용 설명서의 조직 생성을 참조하세요.

AWS Organizations를 사용하여 조직 내 모든 계정을 중앙에서 보고 관리할 수 있습니다. 조직은 관리 계정 하나와 0개 이상의 멤버 계정을 갖습니다. 위에는 루트, 아래에는 조직 단위(OU)가 있는 나무형 계층 구조로 계정을 조직할 수 있습니다. 각 계정은 루트 아래 바로 배치하거나, 계층 구조 내의 OU 중 하나에 배치할 수 있습니다. OU는 특정 계정을 담는 컨테이너입니다. 예를 들어, 재무 운영과 관련된 모든 계정이 포함된 재무 OU를 만들 수 있습니다.

위임된 Security Hub CSPM 관리자 선택에 대한 권장 사항

수동 초대 프로세스에서 관리자 계정이 있고 계정 관리로 전환하는 경우 해당 계정을 위임된 Security Hub CSPM 관리자로 지정하는 AWS Organizations것이 좋습니다.

Security Hub CSPM API와 콘솔은 조직 관리 계정을 위임된 Security Hub CSPM 관리자가 되도록 허용하지만 두 개의 다른 계정을 선택하는 것이 좋습니다. 이를 권장하는 이유는 청구 내용을 관리하기 위해 조직 관리 계정에 액세스할 수 있는 사용자는 보안 관리를 위해 Security Hub CSPM에 액세스해야 하는 사용자와 다를 수 있기 때문입니다.

여러 리전에서 동일한 위임된 관리자를 사용하는 것이 좋습니다. 중앙 구성을 선택하는 경우, Security Hub CSPM은 홈 리전 및 연결된 모든 리전에서 동일한 위임된 관리자를 자동으로 지정합니다.

위임된 관리자를 구성하기 위한 권한 확인

위임된 Security Hub CSPM 관리자 계정을 지정 및 제거하려면 조직 관리 계정은 Security Hub CSPM에서 `EnableOrganizationAdminAccount` 및 `DisableOrganizationAdminAccount` 작업에 대한 권한이 필요합니다. Organizations 관리 계정은 Organizations에 대한 관리자 권한도 가지고 있어야 합니다.

필요한 모든 권한을 부여하려면 다음과 같은 Security Hub CSPM 관리형 정책을 조직 관리 계정의 IAM 위탁자에 연결하세요.

- AWSSecurityHubFullAccess
- AWSSecurityHubOrganizationsAccess

## 위임 관리자 지정

위임된 Security Hub CSPM 관리자 계정을 지정하려면 Security Hub CSPM 콘솔, Security Hub CSPM API 또는 AWS CLI를 사용할 수 있습니다. Security Hub CSPM은 현재 AWS 리전에서만 위임된 관리자를 설정하므로 다른 리전에서 작업을 반복해야 합니다. 중앙 구성을 사용하기 시작하면 Security Hub CSPM은 홈 리전 및 연결된 리전에 동일한 위임된 관리자를 자동으로 설정합니다.

조직 관리 계정은 위임된 Security Hub CSPM 관리자 계정을 지정하기 위해 Security Hub CSPM을 활성화하지 않아도 됩니다.

조직 관리 계정은 Security Hub CSPM 관리자 계정이 아닌 것이 좋습니다. 하지만, 조직 관리 계정을 Security Hub CSPM 위임된 관리자로 선택하는 경우, 관리 계정에 Security Hub CSPM이 활성화되어 있어야 합니다. 관리 계정에 Security Hub CSPM이 활성화되어 있지 않은 경우, Security Hub CSPM을 수동으로 활성화해야 합니다. 조직 관리 계정에서는 Security Hub CSPM을 자동으로 활성화할 수 없습니다.

다음 방법 중 하나를 사용하여 위임된 Security Hub CSPM 관리자를 지정해야 합니다. Organizations API를 사용하여 Security Hub CSPM 위임된 관리자를 지정하면 Security Hub CSPM에 반영되지 않습니다.

원하는 방법을 선택하고 단계에 따라 Security Hub CSPM 위임된 관리자 계정을 지정합니다.

Security Hub CSPM console

온보딩 중에 Security Hub 위임된 관리자를 지정하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. Security Hub CSPM으로 이동을 선택합니다. 조직 관리 계정에 로그인하라는 메시지가 표시됩니다.
3. 위임된 관리자 지정 페이지의 위임된 관리자 계정 섹션에서 위임된 관리자 계정을 지정합니다. 다른 AWS 보안 및 규정 준수 서비스에 설정한 것과 동일한 위임된 관리자를 선택하는 것이 좋습니다.
4. 위임된 관리자 설정을 선택합니다. 중앙 구성으로 온보딩을 계속하려면 위임된 관리자 계정(아직 로그인하지 않은 경우)에 로그인하라는 메시지가 표시됩니다. 중앙 구성을 시작하지 않으려는 경우, 취소를 선택하세요. 위임된 관리자가 설정되었지만 아직 중앙 구성을 사용하고 있지 않습니다.

설정 페이지에서 위임된 Security Hub 관리자를 지정하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. Security Hub CSPM 탐색 창에서 설정을 선택합니다. 그리고 일반을 선택합니다.
3. Security Hub CSPM 관리자 계정이 현재 할당되어 있는 경우, 새로운 계정을 지정하려면 먼저 현재 계정을 제거해야 합니다.

   현재 계정을 제거하려면 위임된 관리자에서 제거를 선택합니다.
4. Security Hub CSPM 관리자 계정으로 지정할 계정의 계정 ID를 입력합니다.

   모든 리전에 동일한 Security Hub CSPM 관리자 계정을 지정해야 합니다. 다른 리전에서 지정된 계정과 다른 계정을 지정하는 경우, 콘솔이 오류를 반환합니다.
5. 위임을 선택합니다.

Security Hub CSPM API,AWS CLI

조직 관리 계정에서 Security Hub CSPM API의 EnableOrganizationAdminAccount 작업을 사용합니다. AWS CLI을(를) 사용하는 경우, enable-organization-admin-account 명령을 실행합니다. 위임된 Security Hub CSPM 관리자의 AWS 계정 ID를 입력합니다.

다음 예제에서는 위임된 Security Hub CSPM 관리자를 지정합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub enable-organization-admin-account --admin-account-id 123456789012
```

위임된 관리자 제거 또는 변경

조직 관리 계정만 위임된 Security Hub CSPM 관리자 계정을 제거할 수 있습니다.

위임된 Security Hub CSPM 관리자 계정을 변경하려면 먼저 현재 위임된 관리자 계정을 제거하고 새로운 관리자 계정을 지정해야 합니다.

> **Warning**
>
> 중앙 구성을 사용하는 경우, Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용하여 위임된 관리자 계정을 변경하거나 제거할 수 없습니다. 조직 관리 계정이 AWS Organizations콘솔 또는 AWS OrganizationsAPIs를 사용하여 위임된 Security Hub CSPM 관

리자를 변경하거나 제거하는 경우 Security Hub CSPM은 자동으로 중앙 구성을 중지하고 구성 정책 및 정책 연결을 삭제합니다. 멤버 계정은 위임된 관리자가 변경되거나 제거되기 전의 구성을 유지합니다.

Security Hub CSPM 콘솔을 사용하여 한 리전에서 위임된 관리자를 제거하면 모든 리전에서 자동으로 제거됩니다.

Security Hub CSPM API는 API 직접 호출 또는 명령이 실행된 리전에서만 위임된 Security Hub CSPM 관리자 계정을 제거합니다. 다른 리전에서도 이 작업을 반복해야 합니다.

Organizations API를 사용하여 위임된 Security Hub CSPM 관리자 계정을 제거하는 경우 모든 리전에서 자동으로 제거됩니다.

위임된 관리자 제거(조직 API,AWS CLI)

Organizations를 사용하여 모든 리전에서 Security Hub CSPM 위임된 관리자를 제거할 수 있습니다.

중앙 구성을 사용하여 계정을 관리하는 경우, 위임된 관리자 계정을 제거하면 구성 정책과 정책 연결이 삭제됩니다. 멤버 계정은 위임된 관리자가 변경되거나 제거되기 전의 구성을 유지합니다. 하지만 제거된 위임된 관리자 계정으로는 더 이상 이러한 계정을 관리할 수 없습니다. 이러한 계정은 각 리전에서 별도로 구성해야 하는 자체 관리형 계정이 됩니다.

원하는 방법을 선택하고 지침에 따라 위임된 Security Hub CSPM 관리자 계정을 제거합니다AWS Organizations.

Organizations API,AWS CLI

Security Hub CSPM 위임된 관리자를 제거하려면

조직 관리 계정에서 Organizations API의 DeregisterDelegatedAdministrator 작업을 사용합니다. AWS CLI을(를) 사용하는 경우, deregister-delegated-administrator 명령을 실행합니다. 위임된 관리자 계정의 계정 ID와 Security Hub CSPM의 서비스 위탁자인 `securityhub.amazonaws.com`을 입력합니다.

다음 예제는 위임된 Security Hub CSPM 관리자를 제거합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

위임된 관리자 제거(Security Hub CSPM 콘솔)

Security Hub CSPM 콘솔을 사용하여 모든 리전에서 위임된 Security Hub CSPM 관리자를 제거할 수 있습니다.

Security Hub CSPM 위임된 관리자 계정이 제거되면 멤버 계정이 제거된 Security Hub CSPM 위임된 관리자 계정에서 연결 해제됩니다.

멤버 계정에는 여전히 Security Hub CSPM이 활성화되어 있습니다. 이러한 계정은 새로운 Security Hub CSPM 관리자가 멤버 계정으로 활성화하기 전까지는 독립형 계정이 됩니다.

조직 관리 계정이 Security Hub CSPM에서 활성화된 계정이 아닌 경우, Security Hub CSPM에 오신 것을 환영합니다 페이지의 옵션을 사용하세요.

Security Hub CSPM에 오신 것을 환영합니다 페이지에서 위임된 Security Hub CSPM 관리자 계정을 제거하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. Security Hub로 이동을 선택합니다.
3. 위임된 관리자에서 제거를 선택합니다.

조직 관리 계정이 Security Hub에서 활성화된 계정인 경우, 설정 페이지의 일반 탭에 있는 옵션을 사용하세요.

설정 페이지에서 Security Hub CSPM 위임된 관리자를 제거하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. Security Hub CSPM 탐색 창에서 설정을 선택합니다. 그리고 일반을 선택합니다.
3. 위임된 관리자에서 제거를 선택합니다.

위임된 관리자 제거(Security Hub CSPM API,AWS CLI)

에 대한 Security Hub CSPM API 또는 Security Hub CSPM 작업을 사용하여 위임된 Security Hub CSPM 관리자를 AWS CLI제거할 수 있습니다. 이러한 방법 중 하나를 사용하여 위임된 관리자를 제거하면 API 호출 또는 명령이 실행된 리전에서만 제거됩니다. Security Hub CSPM은 다른 리전을 업데이트하지 않으며에서 위임된 관리자 계정을 제거하지 않습니다AWS Organizations.

원하는 방법을 선택하고 다음 단계에 따라 Security Hub CSPM으로 위임된Security Hub CSPM 관리자 계정을 제거하세요.

Security Hub CSPM API,AWS CLI

Security Hub CSPM 위임된 관리자를 제거하려면

조직 관리 계정에서 Security Hub CSPM API의 DisableOrganizationAdminAccount 작업을 사용합니다. 를 사용하는 경우 disable-organization-admin-account 명령을 AWS CLI실행합니다. 위임된 Security Hub CSPM 관리자의 계정 ID를 입력합니다.

다음 예제는 위임된 Security Hub CSPM 관리자를 제거합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

와의 Security Hub CSPM 통합 비활성화AWS Organizations

AWS Organizations조직이 AWSSecurity Hub CSPM과 통합되면 Organizations 관리 계정은 나중에 통합을 비활성화할 수 있습니다. Organizations 관리 계정의 사용자는 AWS Organizations에서 Security Hub CSPM에 대한 신뢰할 수 있는 액세스를 비활성화하여 이를 수행할 수 있습니다.

Security Hub CSPM에 대한 신뢰할 수 있는 액세스를 비활성화하면 다음과 같은 결과가 발생합니다.

- Security Hub CSPM은 신뢰할 수 있는 서비스로서 상태를 잃습니다AWS Organizations.
- Security Hub CSPM 위임된 관리자 계정은 모든 AWS 리전에서 모든 Security Hub CSPM 멤버 계정의 Security Hub CSPM 설정, 데이터 및 리소스에 대한 액세스 권한을 상실합니다.
- 중앙 구성을 사용하고 있었다면 Security Hub CSPM은 조직에서 중앙 구성 사용을 자동으로 중지합니다. 구성 정책 및 정책 연결이 삭제됩니다. 계정은 신뢰할 수 있는 액세스를 비활성화하기 전에 사용했던 구성을 유지합니다.
- 모든 Security Hub CSPM 멤버 계정은 독립형 계정이 되며 현재 설정을 유지합니다. Security Hub CSPM이 하나 이상의 리전에서 멤버 계정에 대해 활성화된 경우, Security Hub CSPM은 해당 리전에서 해당 계정을 계속 사용할 수 있습니다. 활성화된 표준 및 제어 역시 변경되지 않습니다. 이러한 설정은 각 계정 및 리전에서 개별적으로 변경할 수 있습니다. 하지만 계정은 더 이상 어떤 리전의 위임된 관리자와도 연결되지 않습니다.

신뢰할 수 있는 서비스 액세스를 비활성화한 결과에 대한 자세한 내용은 AWS Organizations사용 설명서의 다른 AWS Organizations와 함께 사용을AWS 서비스 참조하세요.

신뢰할 수 있는 액세스를 비활성화하려면 AWS Organizations콘솔, Organizations API 또는를 사용할 수 있습니다AWS CLI. Organizations 관리 계정의 사용자만 Security Hub CSPM에 대한 신뢰할 수 있

는 서비스 액세스를 비활성화할 수 있습니다. 필요한 권한에 대한 자세한 내용은 AWS Organizations 사용 설명서의 신뢰할 수 있는 액세스를 비활성화하는 데 필요한 권한을 참조하세요.

신뢰할 수 있는 액세스를 비활성화하기 전에 조직의 위임된 관리자와 협력하여 멤버 계정에서 Security Hub CSPM을 비활성화하고 해당 계정에서 Security Hub CSPM 리소스를 정리하는 것이 좋습니다.

원하는 방법을 선택하고 단계에 따라 Security Hub CSPM에 대한 신뢰할 수 있는 액세스를 비활성화하세요.

Organizations console

Security Hub CSPM에 대한 신뢰할 수 있는 액세스를 비활성화하려면

1. AWS Organizations관리 계정의 자격 증명을 AWS Management Console사용하여에 로그인합니다.
2. https://console.aws.amazon.com/organizations/에서 Organizations 콘솔을 엽니다.
3. 탐색 창에서 서비스를 선택합니다.
4. 통합 서비스에서 AWS Security Hub CSPM을 선택합니다.
5. 신뢰할 수 있는 액세스 비활성화를 선택합니다.
6. 신뢰할 수 있는 액세스를 비활성화할지 확인합니다.

Organizations API

Security Hub CSPM에 대한 신뢰할 수 있는 액세스를 비활성화하려면

AWS OrganizationsAPI의 DisableAWSServiceAccess 작업을 호출합니다. `ServicePrincipal` 파라미터에서 Security Hub CSPM 서비스 위탁자(`securityhub.amazonaws.com`)를 지정합니다.

AWS CLI

Security Hub CSPM에 대한 신뢰할 수 있는 액세스를 비활성화하려면

AWS OrganizationsAPI의 disable-aws-service-access 명령을 실행합니다. `service-principal` 파라미터에서 Security Hub CSPM 서비스 위탁자(`securityhub.amazonaws.com`)를 지정합니다.

예:

```
aws organizations disable-aws-service-access --service-principal
 securityhub.amazonaws.com
```

## 새로운 조직 계정에서 Security Hub CSPM 자동 활성화

새 계정이 조직에 가입하면 AWSSecurity Hub CSPM 콘솔의 계정 페이지에 있는 목록에 추가됩니다. 조직 계정의 경우, 유형은 조직별입니다. 기본적으로 새로운 계정은 조직에 가입할 때 Security Hub CSPM 멤버가 되지 않습니다. 해당 멤버의 상태는 멤버가 아님입니다. 위임된 관리자 계정은 새로운 계정을 자동으로 추가하고 조직에 가입할 때 Security Hub CSPM을 이 계정에 멤버로 활성화할 수 있습니다.

> **Note**
>
> 많은 AWS 리전가 기본적으로에 대해 활성화되어 있지만 특정 리전을 수동으로 활성화AWS 계정해야 합니다. 이 문서에서는 이러한 리전을 옵트인 리전이라고 합니다. 옵트인 리전의 새로운 계정에서 Security Hub CSPM을 자동 활성화하려면 계정에 해당 리전이 먼저 활성화되어 있어야 합니다. 계정 소유자만 옵트인 리전을 활성화할 수 있습니다. 옵트인 리전에 대한 자세한 내용은 계정에서 사용할 수 있는 지정을 참조AWS 리전하세요.

이 프로세스는 중앙 구성(권장)을 사용하는지 로컬 구성을 사용하는지에 따라 달라집니다.

새로운 조직 계정 자동 활성화(중앙 구성)

중앙 구성을 사용하는 경우, Security Hub CSPM이 활성화된 구성 정책을 생성하여 새로운 조직 계정과 기존 조직 계정에서 Security Hub CSPM을 자동으로 활성화할 수 있습니다. 그런 다음 구성 정책을 특정 계정 및 OU(조직 단위) 또는 루트와 연결할 수 있습니다.

Security Hub CSPM이 활성화된 구성 정책을 특정 OU와 연결하면 해당 OU에 속하는 모든 계정(기존 및 신규)에서 Security Hub CSPM이 자동으로 활성화됩니다. OU에 속하지 않는 새로운 계정은 자체 관리되며 Security Hub CSPM이 자동으로 활성화되지 않습니다. Security Hub CSPM이 활성화된 구성 정책을 루트와 연결하면 조직에 가입한 모든 계정(기존 및 새로운)에서 Security Hub CSPM이 자동으로 활성화됩니다. 단, 계정이 적용 또는 상속을 통해 다른 정책을 사용하거나 자체 관리하는 경우는 예외입니다.

구성 정책에서는 OU에서 활성화해야 하는 보안 표준 및 제어를 정의할 수도 있습니다. 활성화된 표준에 대한 제어 조사 결과를 생성하려면 OU의 계정이 필수 리소스를 기록하도록 AWS Config활성화하고 구성해야 합니다. AWS Config녹음에 대한 자세한 내용은 활성화 및 구성을AWS Config 참조하세요.

구성 정책 생성에 대한 지침은 구성 정책 생성 및 연결 섹션을 참조하세요.

새로운 조직 계정 자동 활성화(로컬 구성)

로컬 구성을 사용하고 자동 활성화를 켜면 Security Hub CSPM은 새로운 조직 계정을 멤버로 추가하고 현재 리전의 해당 계정에서 Security Hub CSPM을 활성화합니다. 다른 리전은 영향을 받지 않습니다. 또한 자동 활성화 기능을 켜도 이미 멤버 계정으로 추가된 경우를 제외하고 기존 조직 계정에서 Security Hub CSPM은 활성화되지 않습니다.

자동 활성화 기능을 켜면, 조직에 가입할 때 현재 리전의 새로운 계정의 기본 보안 표준이 자동으로 활성화됩니다. 기본 표준은 AWSFoundational Security Best Practices(FSBP) 및 Center for Internet Security(CIS)AWSFoundations Benchmark v1.2.0입니다. 기본 표준은 변경할 수 없습니다. 조직 전체에서 다른 표준을 사용하거나 일부 계정 및 OU에 표준을 적용하려면 중앙 구성을 사용하는 것이 좋습니다.

기본 표준(및 기타 활성화된 표준)에 대한 제어 조사 결과를 생성하려면 조직의 계정에서 필요한 리소스를 기록하도록 AWS Config활성화하고 구성해야 합니다. AWS Config녹음에 대한 자세한 내용은 활성화 및 구성을AWS Config 참조하세요.

원하는 방법을 선택하고 단계에 따라 새로운 조직 계정에서 Security Hub CSPM을 자동으로 활성화합니다. 이 지침은 로컬 구성을 사용하는 경우에만 적용됩니다.

Security Hub CSPM console

새로운 조직 계정을 Security Hub CSPM 멤버로 자동으로 활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. Security Hub CSPM 탐색 창의 설정에서 구성을 선택합니다.
3. 계정 섹션에서 계정 자동 활성화를 켭니다.

Security Hub CSPM API

새로운 조직 계정을 Security Hub CSPM 멤버로 자동으로 활성화하려면

위임된 관리자 계정에서 `UpdateOrganizationConfiguration` API를 호출합니다. 새로운 조직 계정에서 Security Hub CSPM을 자동으로 활성화하려면 `AutoEnable` 필드를 `true`로 설정합니다.

AWS CLI

새로운 조직 계정을 Security Hub CSPM 멤버로 자동으로 활성화하려면

위임된 관리자 계정에서 update-organization-configuration 명령을 실행합니다. 새로운 조직 계정에서 Security Hub CSPM을 자동으로 활성화하는 auto-enable 파라미터를 포함합니다.

```
aws securityhub update-organization-configuration --auto-enable
```

## 새로운 조직 계정에서 Security Hub CSPM 수동 활성화

새로운 조직 계정이 조직에 가입할 때 자동으로 Security Hub CSPM을 활성화하지 않은 경우, 조직에 가입한 후 해당 계정에서 Security Hub CSPM을 수동으로 활성화할 수 있습니다. 또한 이전에 조직에서 연결 해제AWS 계정한에서 Security Hub CSPM을 수동으로 활성화해야 합니다.

> **Note**
>
> 중앙 구성을 사용하는 경우, 이 섹션이 적용되지 않습니다. 중앙 구성을 사용하는 경우, 지정된 멤버 계정 및 조직 단위(OU)에서 Security Hub CSPM을 활성화하는 구성 정책을 만들 수 있습니다. 또한 해당 계정과 OU에서 특정 표준 및 제어를 활성화할 수 있습니다.

이미 다른 조직의 멤버 계정인 경우, 해당 계정에서 Security Hub CSPM을 활성화할 수 없습니다.

또한 현재 일시 중지된 계정에서는 Security Hub CSPM을 활성화할 수 없습니다. 일시 중지된 계정의 서비스를 활성화하려고 하면 계정 상태가 계정 일시 중단됨으로 변경됩니다.

- 계정에 Security Hub CSPM이 활성화되지 않은 경우, 해당 계정에서 Security Hub CSPM이 활성화됩니다. 기본 보안 표준을 끄지 않는 한 AWS기본 보안 모범 사례(FSBP) 표준 및 CISAWS Foundations Benchmark v1.2.0도 계정에서 활성화됩니다.

  이에 대한 예외는 Organizations 관리 계정입니다. Organizations 관리 계정에서는 Security Hub CSPM을 자동으로 활성화할 수 없습니다. Organizations 관리 계정을 멤버 계정으로 활성화하려면 먼저 Organizations 관리 계정에서 수동으로 Security Hub CSPM을 활성화해야 합니다.
- 계정에 이미 Security Hub CSPM이 활성화되어 있는 경우, Security Hub CSPM은 계정에 다른 변경 사항을 적용하지 않습니다. 멤버십만 활성화합니다.

Security Hub CSPM이 제어 조사 결과를 생성하려면 멤버 계정이 필요한 리소스를 기록하도록 AWS Config활성화하고 구성해야 합니다. 자세한 내용은 AWS Config 설정 및 구성을 참조하세요.

원하는 방법을 선택하고 단계에 따라 조직 계정을 Security Hub CSPM 멤버 계정으로 활성화합니다.

Security Hub CSPM console

조직 계정을 Security Hub CSPM 멤버로 수동으로 활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. Security Hub CSPM 탐색 창의 설정에서 구성을 선택합니다.
3. 계정 목록에서 활성화할 각 조직 계정을 선택합니다.
4. 작업을 선택하고 멤버 추가를 선택합니다.

Security Hub CSPM API

조직 계정을 Security Hub CSPM 멤버로 수동으로 활성화하려면

위임된 관리자 계정에서 `CreateMembers` API를 호출합니다. 활성화할 각 계정의 계정 ID를 입력합니다.

수동 초대 프로세스와 달리 조직 계정을 활성화하는 데 `CreateMembers`을(를) 호출하는 경우, 초대를 보낼 필요가 없습니다.

AWS CLI

조직 계정을 Security Hub CSPM 멤버로 수동으로 활성화하려면

위임된 관리자 계정에서 `create-members` 명령을 실행합니다. 활성화할 각 계정의 계정 ID를 입력합니다.

수동 초대 프로세스와 달리 조직 계정을 활성화하는 데 `create-members`을(를) 실행하는 경우, 초대를 보낼 필요가 없습니다.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

예제

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

## 조직에서 Security Hub CSPM 멤버 계정 연결 해제

AWSSecurity Hub CSPM 멤버 계정의 조사 결과 수신 및 보기를 중지하려면 조직에서 멤버 계정의 연결을 해제하면 됩니다.

> **Note**
>
> 중앙 구성을 사용하는 경우, 연결 해제가 다르게 작동합니다. 중앙에서 관리되는 하나 이상의 멤버 계정에서 Security Hub CSPM을 비활성화하는 구성 정책을 만들 수 있습니다. 그 이후에도 이러한 계정은 여전히 조직의 일부이지만 Security Hub CSPM 조사 결과를 생성하지는 않습니다. 중앙 구성을 사용하지만 수동으로 초대된 멤버 계정이 있는 경우, 수동으로 초대된 계정을 하나 이상 연결 해제할 수 있습니다.

를 사용하여 관리되는 멤버 계정은 관리자 계정에서 계정의 연결을 해제할 AWS Organizations수 없습니다. 관리자 계정만 멤버 계정 연결을 해제할 수 있습니다.

멤버 계정을 연결 해제해도 계정은 해지되지 않습니다. 대신 조직에서 멤버 계정을 제거합니다. 연결 해제된 멤버 계정은 더 이상 Security Hub CSPM 통합에서 관리하지 AWS 계정않는 독립 실행형 계정이 됩니다AWS Organizations.

원하는 방법을 선택하고 단계에 따라 조직에서 멤버 계정을 연결 해제하세요.

Security Hub CSPM console

조직에서 멤버 계정을 연결 해제하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   위임된 관리자 계정의 보안 인증 정보를 사용하여 로그인합니다.
2. 탐색 창의 설정에서 구성을 선택합니다.
3. 계정 섹션에서 연결을 해제하려는 계정을 선택합니다. 중앙 구성을 사용하는 경우, 수동으로 초대된 계정을 선택하여 `Invitation accounts` 탭에서 연결을 해제할 수 있습니다. 이 탭은 중앙 구성을 사용하는 경우에만 표시됩니다.
4. 작업을 선택한 다음 계정 연결 해제를 선택합니다.

Security Hub CSPM API

조직에서 멤버 계정을 연결 해제하려면

위임된 관리자 계정에서 `DisassociateMembers` API를 호출합니다. 멤버 계정의 연결을 해제하려면 AWS 계정IDs를 제공해야 합니다. 멤버 계정 목록을 보려면 `ListMembers` API를 호출합니다.

AWS CLI

조직에서 멤버 계정을 연결 해제하려면

위임된 관리자 계정에서 `>disassociate-members` 명령을 실행합니다. 멤버 계정의 연결을 해제하려면 AWS 계정IDs를 제공해야 합니다. 멤버 계정 목록을 보려면 `>list-members` 명령을 실행합니다.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

예제

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

AWS Organizations콘솔AWS CLI, 또는AWSSDKs를 사용하여 조직에서 멤버 계정의 연결을 해제할 수도 있습니다. 자세한 내용은 AWS Organizations 사용 설명서의 조직에서 멤버 계정 제거를 참조하세요.

## Security Hub CSPM에서 초대를 통한 계정 관리

AWSSecurity Hub CSPM을와 통합AWS Organizations하거나 멤버십 초대를 수동으로 보내고 수락하여 두 가지 방법으로 여러 Security Hub CSPM 계정을 중앙에서 관리할 수 있습니다. 독립 실행형 계정이 있거나와 통합되지 않은 경우 수동 프로세스를 사용해야 합니다AWS Organizations. 수동 계정 관리에서는 Security Hub CSPM 관리자가 계정을 멤버로 초대합니다. 예비 멤버가 초대를 수락하면 관리자-멤버 관계가 성립됩니다. Security Hub CSPM 관리자 계정은 최대 1,000개의 초대 기반 멤버 계정에 대한 Security Hub CSPM을 관리할 수 있습니다.

> **Note**
>
> Security Hub CSPM에서 초대 기반 조직을 만든 경우, 나중에 대신 AWS Organizations를 사용하도록 전환할 수 있습니다. 멤버 계정이 두 개 이상인 경우 Security Hub CSPM 초대 AWS

Organizations대신를 사용하여 멤버 계정을 관리하는 것이 좋습니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 단원을 참조하세요.

수동 초대 프로세스를 통해 초대하는 계정에 대해 결과와 기타 데이터에 대한 교차 리전 집계를 사용할 수 있습니다. 하지만 리전 간 집계가 작동하려면 관리자가 집계 리전과 연결된 모든 리전에서 멤버 계정을 초대해야 합니다. 또한 관리자가 멤버 계정의 조사 결과를 볼 수 있도록 멤버 계정에는 집계 영역과 연결된 모든 리전에서 Security Hub CSPM이 활성화되어 있어야 합니다.

구성 정책은 수동으로 초대된 멤버 계정에는 지원되지 않습니다. 대신 수동 초대 프로세스를 사용할 AWS 리전때 각 멤버 계정과에서 Security Hub CSPM 설정을 별도로 구성해야 합니다.

또한 조직에 속하지 않은 계정에 대해서는 수동 초대 기반 프로세스를 사용해야 합니다. 예를 들어, 조직에 테스트 계정을 포함하지 않을 수도 있습니다. 또는 여러 조직의 계정을 하나의 Security Hub CSPM 관리자 계정으로 통합할 수도 있습니다. Security Hub CSPM 관리자 계정은 다른 조직에 속한 계정으로 초대를 보내야 합니다.

Security Hub CSPM 콘솔의 구성 페이지에서 초대를 통해 추가된 계정이 초대 계정 탭에 나열됩니다. 중앙 구성을 사용하지만 조직 외부 계정을 초대하는 경우, 이 탭에서 초대 기반 계정의 조사 결과를 볼 수 있습니다. 하지만 Security Hub CSPM 관리자는 구성 정책을 사용하여 여러 리전의 초대 기반 계정을 구성할 수 없습니다.

이 섹션의 주제에서는 초대를 통해 멤버 계정을 관리하는 방법을 설명합니다.

주제

- Security Hub CSPM에서 멤버 계정 추가 및 초대
- Security Hub CSPM 멤버 계정 초대에 응답
- Security Hub CSPM에서 멤버 계정 연결 해제
- Security Hub CSPM에서 멤버 계정 삭제
- Security Hub CSPM 관리자 계정에서 연결 해제
- Security Hub CSPM에서 계정을 관리하기 위해 Organizations로 전환

# Security Hub CSPM에서 멤버 계정 추가 및 초대

> **Note**
>
> Security Hub CSPM 초대 AWS Organizations대신를 사용하여 멤버 계정을 관리하는 것이 좋습니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 단원을 참조하세요.

계정은 AWSSecurity Hub CSPM 멤버 계정 가입 초대를 수락하는 계정의 Security Hub CSPM 관리자가 됩니다.

다른 계정으로부터 온 초대를 수락하면 사용자 계정이 멤버 계정이 되고 해당 계정이 귀하의 관리자가 됩니다.

사용자 계정이 관리자 계정인 경우, 멤버 계정이 되기 위한 초대를 수락할 수 없습니다.

멤버 계정 추가는 다음과 같은 단계로 구성됩니다.

1. 관리자 계정이 멤버 계정 목록에 멤버 계정을 추가합니다.
2. 관리자 계정이 멤버 계정에 초대를 보냅니다.
3. 멤버 계정이 초대를 수락합니다.

## 멤버 계정 추가

Security Hub CSPM 콘솔에서 멤버 계정 목록에 계정을 추가할 수 있습니다. Security Hub CSPM 콘솔에서 계정을 개별적으로 선택하거나 계정 정보가 포함된 `.csv` 파일을 업로드할 수 있습니다.

계정마다 계정 ID와 이메일 주소를 제공해야 합니다. 이메일 주소는 계정의 보안 문제에 대해 문의할 수 있는 이메일 주소여야 합니다. 이 이메일 주소는 계정 인증에 사용되지 않습니다.

원하는 방법을 선택하고 단계에 따라 멤버 계정을 추가하세요.

### Security Hub CSPM console

멤버 계정 목록에 계정을 추가하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.

2. 왼쪽 창에서 설정을 선택합니다.
3. 설정 페이지에서 계정을 선택하고 계정 추가를 선택합니다. 그런 다음에는 계정을 개별적으로 추가하거나 계정 목록이 포함된 .csv 파일을 업로드할 수 있습니다.
4. 이 계정을 선택하려면 다음 중 하나를 수행하세요.

   - 개별로 계정을 추가하려면 계정 입력에서 추가할 계정의 계정 ID 및 이메일 주소를 입력하고 추가를 선택합니다.

     각 계정마다 이 절차를 반복합니다.

   - 쉼표로 구분된 값(.csv) 파일을 사용하여 복수 계정을 추가하려면 먼저 파일을 생성해야 합니다. 파일에는 추가할 각 계정의 계정 ID와 이메일 주소가 포함되어야 합니다.

     .csv 목록에는 계정이 한 줄에 하나씩 표시되어야 합니다. .csv 파일의 첫 번째 줄에는 헤더가 포함되어야 합니다. 헤더에서 첫 번째 열은 **Account ID**이고, 두 번째 열은 **Email**입니다.

     이어지는 각 줄에는 추가하려는 계정에 대한 계정 ID 및 유효한 이메일 주소가 포함되어야 합니다.

     다음은 텍스트 편집기에서 보는 .csv 파일의 예제입니다.

     ```
     Account ID,Email
     111111111111,user@example.com
     ```

     스프레드시트 프로그램에서는 필드가 별도의 열에 표시됩니다. 기본 형식은 여전히 쉼표로 구분됩니다. 계정 ID의 형식은 소수점이 없는 숫자로 지정해야 합니다. 예를 들어, 계정 ID 444455556666은 444455556666.0으로 형식을 지정할 수 없습니다. 또한, 숫자 형식으로 인해 계정 ID에서 앞에 오는 0이 제거되지 않도록 해야 합니다.

     파일을 선택하려면 콘솔에서 목록 업로드(.csv)를 선택합니다. 그런 다음 찾아보기를 선택합니다.

     파일을 선택한 후 계정 추가를 선택합니다.
5. 계정 추가를 완료한 후 추가할 계정에서 다음을 선택합니다.

Security Hub CSPM API

멤버 계정 목록에 계정을 추가하려면

관리자 계정에서 CreateMembers API를 호출합니다. 추가할 각 멤버 계정에 대해 AWS 계정ID를 제공해야 합니다.

AWS CLI

멤버 계정 목록에 계정을 추가하려면

관리자 계정에서 create-members 명령을 실행합니다. 추가할 각 멤버 계정에 대해 AWS 계정ID를 제공해야 합니다.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

예제

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"},
 {"AccountId": "123456789222"}]'
```

멤버 계정 초대

멤버 계정을 추가한 후 멤버 계정에 초대를 전송합니다. 관리자와의 연결이 해제된 계정에 초대를 다시 보낼 수도 있습니다.

Security Hub CSPM console

예비 멤버 계정을 초대하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.
2. 탐색 창에서 설정을 선택한 다음 계정을 선택합니다.
3. 초대한 계정의 상태 열 값에서 초대를 선택합니다.
4. 확인하라는 메시지가 나타나면 초대를 선택합니다.

> **Note**
>
> 연결이 해제된 계정에 초대를 다시 보내려면 계정 페이지에서 연결이 해제된 각 계정을 선택합니다. 작업에서 초대 재전송을 선택합니다.

Security Hub CSPM API

예비 멤버 계정을 초대하려면

관리자 계정에서 `InviteMembers` API를 호출합니다. 초대할 각 계정에 대해 AWS 계정ID를 제공해야 합니다.

AWS CLI

예비 멤버 계정을 초대하려면

관리자 계정에서 `invite-members` 명령을 실행합니다. 초대할 각 계정에 대해 AWS 계정ID를 제공해야 합니다.

```
aws securityhub invite-members --account-ids <accountIDs>
```

예제

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

## Security Hub CSPM 멤버 계정 초대에 응답

> **Note**
>
> Security Hub CSPM 초대 AWS Organizations대신를 사용하여 멤버 계정을 관리하는 것이 좋습니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 단원을 참조하세요.

AWSSecurity Hub CSPM 멤버 계정 초대를 수락하거나 거부할 수 있습니다.

초대를 수락하는 경우 사용자 계정은 Security Hub CSPM 멤버 계정이 됩니다. 초대를 보낸 계정은 Security Hub CSPM 관리자 계정이 됩니다. 관리자 계정 사용자는 Security Hub CSPM에서 멤버 계정에 대한 조사 결과를 볼 수 있습니다.

초대를 거부하면 관리자 계정의 멤버 계정 목록에 계정이 탈퇴로 표시됩니다.

멤버 계정으로 가입하라는 초대를 수락하거나 거절할 수만 있습니다.

초대를 수락하거나 거절하려면 먼저 Security Hub CSPM을 활성화해야 합니다.

모든 Security Hub CSPM 계정은 모든 리소스를 기록하도록 AWS Config활성화하고 구성해야 합니다. 요구 사항에 대한 자세한 내용은 활성화 및 구성을AWS Config AWS Config참조하세요.

초대 수락

관리자 계정에서 Security Hub CSPM 멤버 계정 초대를 보낼 수 있습니다. 그런 다음 멤버 계정에 로그인한 후 초대를 수락할 수 있습니다.

원하는 방법을 선택하고 단계에 따라 멤버 계정 초대를 수락하세요.

Security Hub CSPM console

멤버십 초대를 수락하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 계정을 선택합니다.
3. 관리자 계정에서 수락을 켠 다음 초대 수락을 선택합니다.

Security Hub CSPM API

멤버십 초대를 수락하려면

`AcceptAdministratorInvitation` API를 호출합니다. 초대 식별자와 관리자 계정의 AWS 계정ID를 제공해야 합니다. 초대에 대한 세부 정보를 검색하려면 `ListInvitations` 작업을 사용하세요.

AWS CLI

멤버십 초대를 수락하려면

`accept-administrator-invitation` 명령을 실행합니다. 초대 식별자와 관리자 계정의 AWS 계정ID를 제공해야 합니다. 초대에 대한 세부 정보를 검색하려면 `list-invitations` 명령을 실행합니다.

```
aws securityhub accept-administrator-invitation --administrator-
id <administratorAccountID> --invitation-id <invitationID>
```

예제

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --
invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

> **Note**
>
> Security Hub CSPM 콘솔은 `AcceptInvitation`을 계속 사용합니다. 결국에는 `AcceptAdministratorInvitation`을(를) 사용하도록 변경됩니다. 이 기능에 대한 액세스를 구체적으로 제어하는 모든 IAM 정책은 계속 `AcceptInvitation`을(를) 사용해야 합니다. 또한, 콘솔이 `AcceptAdministratorInvitation`을(를) 사용하기 시작하면 올바른 권한이 적용되도록 `AcceptAdministratorInvitation`을(를) 정책에 추가해야 합니다.

### 초대 거부

Security Hub CSPM 멤버 계정으로 가입하라는 초대를 수락하거나 거절할 수 있습니다. Security Hub CSPM 콘솔에서 초대를 거부하면 관리자 계정의 멤버 계정 목록에 계정이 탈퇴로 표시됩니다. 탈퇴 상태는 관리자 계정을 사용하여 Security Hub CSPM 콘솔에 로그인할 때만 나타납니다. 그러나 관리자 계정에 로그인하고 초대를 삭제할 때까지 멤버 계정의 콘솔에서 초대는 변경되지 않습니다.

초대를 거부할 때는 초대를 받은 멤버 계정으로 로그인해야 합니다.

원하는 방법을 선택하고 단계에 따라 멤버 계정 초대를 거부하세요.

#### Security Hub CSPM console

멤버십 초대를 거부하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 계정을 선택합니다.
3. 관리자 계정 섹션에서 초대 거부를 선택합니다.

#### Security Hub CSPM API

멤버십 초대를 거부하려면

`DeclineInvitations` API를 호출합니다. 초대를 발행한 관리자 계정의 AWS 계정ID를 제공해야 합니다. 초대에 대한 정보를 보려면 `ListInvitations` 작업을 사용하세요.

AWS CLI

멤버십 초대를 거부하려면

`decline-invitations` 명령을 실행합니다. 초대를 발행한 관리자 계정의 AWS 계정ID를 제공해야 합니다. 초대에 대한 정보를 보려면 `list-invitations` 명령을 실행합니다.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

예제

```
aws securityhub decline-invitations --account-ids "123456789012"
```

## Security Hub CSPM에서 멤버 계정 연결 해제

> **Note**
>
> Security Hub CSPM 초대 AWS Organizations대신를 사용하여 멤버 계정을 관리하는 것이 좋습니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 단원을 참조하세요.

AWSSecurity Hub CSPM 관리자 계정은 멤버 계정의 연결을 해제하여 해당 계정의 조사 결과 수신 및 보기를 중지할 수 있습니다. 멤버 계정을 삭제하기 전에는 멤버 계정 연결을 해제해야 합니다.

멤버 계정을 연결 해제해도 멤버 계정 목록에는 해당 계정이 제거됨(연결 해제됨) 상태인 상태로 남아 있습니다. 멤버 계정의 관리자 계정 정보에서 계정이 제거됩니다.

계정에 대한 조사 결과를 다시 받으려면 초대를 다시 보내면 됩니다. 멤버 계정을 완전히 삭제하려면 멤버 계정을 삭제하면 됩니다.

원하는 방법을 선택하고 단계에 따라 관리자 계정에서 수동으로 초대된 멤버 계정을 연결 해제하세요.

Security Hub CSPM console

수동으로 초대된 멤버 계정을 연결 해제하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.

2. 탐색 창의 설정에서 구성을 선택합니다.
3. 계정 섹션에서 연결을 해제하려는 계정을 선택합니다.
4. 작업을 선택한 다음 계정 연결 해제를 선택합니다.

Security Hub CSPM API

수동으로 초대된 멤버 계정을 연결 해제하려면

관리자 계정에서 `DisassociateMembers` API를 호출합니다. 연결 해제하려는 멤버 계정의 AWS 계정IDs를 제공해야 합니다. 멤버 계정 목록을 보려면 `ListMembers` 작업을 사용하세요.

AWS CLI

수동으로 초대된 멤버 계정을 연결 해제하려면

관리자 계정에서 `disassociate-members` 명령을 실행합니다. 연결 해제하려는 멤버 계정의 AWS 계정IDs를 제공해야 합니다. 멤버 계정 목록을 보려면 `list-members` 명령을 실행합니다.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

예제

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

## Security Hub CSPM에서 멤버 계정 삭제

> **Note**
>
> Security Hub CSPM 초대 AWS Organizations대신를 사용하여 멤버 계정을 관리하는 것이 좋습니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 단원을 참조하세요.

AWSSecurity Hub CSPM 관리자 계정은 초대를 통해 추가된 멤버 계정을 삭제할 수 있습니다. 멤버 계정을 삭제하기 전에는 멤버 계정 연결을 해제해야 합니다.

멤버 계정을 삭제하면 목록에서 완전히 제거됩니다. 계정의 멤버십을 복원하려면 계정을 추가하고 완전히 새로운 멤버 계정인 것처럼 다시 초대해야 합니다.

조직에 속하고 와의 통합을 사용하여 관리되는 계정은 삭제할 수 없습니다AWS Organizations.

원하는 방법을 선택하고 단계에 따라 수동으로 초대된 멤버 계정을 삭제하세요.

Security Hub CSPM console

수동으로 초대된 멤버 계정을 삭제하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   관리자 계정을 사용하여 로그인합니다.
2. 탐색 창에서 설정을 선택한 다음 구성을 선택합니다.
3. 초대 계정 탭을 선택합니다. 그런 다음 삭제할 계정을 선택합니다.
4. 작업을 선택한 후 삭제를 선택합니다. 이 옵션은 계정 연결을 해제한 경우에만 사용할 수 있습니다. 멤버 계정을 삭제하려면 먼저 멤버 계정 연결을 해제해야 합니다.

Security Hub CSPM API

수동으로 초대된 멤버 계정을 삭제하려면

관리자 계정에서 `DeleteMembers` API를 호출합니다. 삭제하려는 멤버 계정의 AWS 계정 ID를 제공해야 합니다. 멤버 계정 목록을 검색하려면 `ListMembers` API를 호출합니다.

AWS CLI

수동으로 초대된 멤버 계정을 삭제하려면

관리자 계정에서 `delete-members` 명령을 실행합니다. 삭제하려는 멤버 계정의 AWS 계정 ID를 제공해야 합니다. 멤버 계정 목록을 검색하려면 `list-members` 명령을 실행합니다.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

예제

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

# Security Hub CSPM 관리자 계정에서 연결 해제

> **Note**
>
> Security Hub CSPM 초대 AWS Organizations대신를 사용하여 멤버 계정을 관리하는 것이 좋습니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 단원을 참조하세요.

초대를 통해 계정을 AWSSecurity Hub CSPM 멤버 계정으로 추가한 경우 관리자 계정에서 멤버 계정의 연결을 해제할 수 있습니다. 멤버 계정을 연결 해제하면, Security Hub CSPM은 계정의 조사 결과를 관리자 계정으로 보내지 않습니다.

와의 통합을 사용하여 관리되는 멤버 계정은 관리자 계정에서 계정의 연결을 해제할 AWS Organizations수 없습니다. Security Hub CSPM 위임된 관리자만 Organizations로 관리하는 멤버 계정을 연결 해제할 수 있습니다.

관리자 계정과의 연결을 끊어도 해당 계정은 관리자 계정의 멤버 목록에 탈퇴 상태로 남아 있습니다. 하지만, 관리자 계정은 사용자의 계정에 대한 조사 결과를 받을 수 없습니다.

관리자 계정과의 연결을 해제한 후에도 멤버로 가입하라는 초대는 아직 남아 있습니다. 나중에 다시 초대를 수락할 수 있습니다.

Security Hub CSPM console

관리자 계정과의 연결을 해제하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 계정을 선택합니다.
3. 관리자 계정 섹션에서 수락을 끄고 업데이트를 선택합니다.

Security Hub CSPM API

관리자 계정과의 연결을 해제하려면

`DisassociateFromAdministratorAccount` API를 호출합니다.

AWS CLI

관리자 계정과의 연결을 해제하려면

disassociate-from-administrator-account 명령을 실행합니다.

```
aws securityhub disassociate-from-administrator-account
```

> **Note**
>
> Security Hub CSPM 콘솔은 DisassociateFromMasterAccount을 계속 사용합니다. 결국에는 DisassociateFromAdministratorAccount을(를) 사용하도록 변경됩니다. 이 기능에 대한 액세스를 구체적으로 제어하는 모든 IAM 정책은 계속 DisassociateFromMasterAccount을(를) 사용해야 합니다. 또한, 콘솔이 DisassociateFromAdministratorAccount을(를) 사용하기 시작하면 올바른 권한이 적용되도록 DisassociateFromAdministratorAccount을(를) 정책에 추가해야 합니다.

## Security Hub CSPM에서 계정을 관리하기 위해 Organizations로 전환

AWSSecurity Hub CSPM에서 계정을 수동으로 관리하는 경우 예비 멤버 계정을 초대하고 각 멤버 계정을 개별적으로 구성해야 합니다AWS 리전.

Security Hub CSPM과를 통합AWS Organizations하면 초대장을 보낼 필요가 없으며 조직에서 Security Hub CSPM을 구성하고 사용자 지정하는 방법을 더 잘 제어할 수 있습니다. 따라서 Security Hub CSPM 초대 대신 AWS Organizations를 사용하여 멤버 계정을 관리하는 것을 권장합니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 단원을 참조하세요.

AWS Organizations통합을 사용하는 결합된 접근 방식을 사용할 수 있지만 조직 외부에 계정을 수동으로 초대할 수도 있습니다. 하지만 Organizations 통합만 사용하는 것이 좋습니다. 여러 계정 및 리전에서 Security Hub CSPM을 관리하는 데 도움이 되는 기능인 중앙 구성은 Organizations와 통합할 때만 사용할 수 있습니다.

이 섹션에서는 AWS Organizations을(를) 통해 수동 초대 기반 계정 관리에서 계정 관리로 전환하는 방법을 설명합니다.

Security Hub CSPM과 통합AWS Organizations

먼저 Security Hub CSPM과를 통합해야 합니다AWS Organizations.

다음 단계를 완료하면 이러한 서비스를 통합할 수 있습니다.

- AWS Organizations에서 조직을 생성합니다. 지침은 AWS Organizations 사용 설명서의 조직 생성을 참조하세요.
- Organizations 관리 계정에서 Security Hub CSPM 위임된 관리자 계정을 지정합니다.

> **Note**
>
> Organizations 관리 계정은 DA 계정으로 설정할 수 없습니다.

자세한 지침은 Security Hub CSPM과 통합AWS Organizations 섹션을 참조하세요.

이전 단계를 완료하면에서 Security Hub CSPM에 대한 신뢰할 수 있는 액세스 권한을 부여합니다AWS Organizations. 또한 이렇게 하면 위임된 관리자 계정의 현재에서 Security Hub CSPMAWS 리전이 활성화됩니다.

위임된 관리자는 주로 조직의 계정을 Security Hub CSPM 멤버 계정으로 추가하여 Security Hub CSPM에서 조직을 관리할 수 있습니다. 관리자는 해당 계정에 대한 특정 Security Hub CSPM 설정, 데이터 및 리소스에 액세스할 수도 있습니다.

Organizations를 사용하여 계정 관리로 전환해도 초대 기반 계정이 자동으로 Security Hub CSPM 멤버가 되지는 않습니다. 새로운 조직에 추가하는 계정만 Security Hub CSPM 멤버가 될 수 있습니다.

통합을 활성화한 후에는 Organizations를 사용하여 계정을 관리할 수 있습니다. 자세한 내용은 를 사용하여 여러 계정에 대한 Security Hub CSPM 관리AWS Organizations 섹션을 참조하세요. 계정 관리는 조직의 구성 유형에 따라 달라집니다.

## Security Hub CSPM에서 관리자 및 멤버 계정별로 허용된 작업

관리자 및 멤버 계정은 다음 표에 나와 있는 AWSSecurity Hub CSPM 작업에 액세스할 수 있습니다. 표에서 값의 의미는 다음과 같습니다.

- 임의 – 이 계정은 동일한 관리자에 속한 모든 계정에 대해 작업을 수행할 수 있습니다.
- 현재 – 이 계정은 해당 계정(현재 로그인되어 있는 계정)에 대해서만 작업을 수행할 수 있습니다.
- 대시(-) – 해당 계정에서 작업을 수행할 수 없음을 나타냅니다.

표에 명시된 대로 허용되는 작업은 AWS Organizations와 통합하는지 여부와 조직에서 사용하는 구성 유형에 따라 달라집니다. 중앙 구성과 로컬 구성의 차이에 대한 자세한 내용은 를 사용하여 계정 관리 AWS Organizations 섹션을 참조하세요.

Security Hub CSPM은 멤버 계정의 조사 결과를 관리자 계정에 복사하지 않습니다. Security Hub CSPM에서는 모든 조사 결과가 특정 리전의 특정 계정에 수집됩니다. 각 리전에서 관리자 계정은 해당 리전의 멤버 계정에 대한 조사 결과를 보고 관리할 수 있습니다.

집계 영역을 설정하는 경우, 관리자 계정은 집계 영역에 복제된 연결된 리전의 멤버 계정에 대한 조사 결과를 보고 관리할 수 있습니다. 교차 리전 집계에 대한 자세한 내용은 교차 리전 집계 활성화를 참조하세요.

다음 표에는 관리자 및 멤버 계정의 기본 권한이 나와 있습니다. 사용자 지정 IAM 정책을 사용하여 Security Hub CSPM 기능에 대한 액세스를 추가로 제한할 수 있습니다. 지침과 예제는 블로그 게시물 Aligning IAM policies to user personas for AWSSecurity Hub CSPM을 참조하세요.

Organizations와 통합하고 중앙 구성을 사용하는 경우, 허용되는 작업

Organizations와 통합하고 중앙 구성을 사용하는 경우, 관리자 및 멤버 계정은 다음과 같이 Security Hub CSPM 작업에 액세스할 수 있습니다.

| 작업 | Security Hub CSPM 위임된 관리자 계정 | 중앙 관리형 멤버 계정 | 자체 관리형 멤버 계정 |
|---|---|---|---|
| Security Hub CSPM 구성 정책 생성 및 관리 | 자체 관리형 및 중앙 관리형 계정의 경우 | – | – |
| 조직 세부 정보 보기 | 임의 | – | – |
| 멤버 계정 연결 해지 | 임의 | – | – |
| 멤버 계정 삭제 | 임의의 비조직 계정 | – | – |
| Security Hub CSPM 비활성화 | 현재 계정 및 중앙 관리형 계정의 경우 | – | 현재(계정을 관리자 계정에서 분리해야 합니다) |
| 조사 결과 및 조사 결과 기록 보기 | 임의 | 현재 | 현재 |
| 조사 결과 업데이트 | 임의 | 현재 | 현재 |
| 인사이트 결과 보기 | 임의 | 현재 | 현재 |

| 작업 | Security Hub CSPM 위임된 관리자 계정 | 중앙 관리형 멤버 계정 | 자체 관리형 멤버 계정 |
|---|---|---|---|
| 제어 기능 세부 정보 보기 | 임의 | 현재 | 현재 |
| 통합 제어 기능에 대한 조사 결과 켜기 또는 끄기 | 임의 | – | – |
| 표준 활성화 및 비활성화 | 현재 계정 및 중앙 관리형 계정의 경우 | – | 현재 |
| 제어 기능 활성화 및 비활성화 | 현재 계정 및 중앙 관리형 계정의 경우 | – | 현재 |
| 통합 활성화 및 비활성화 | 현재 | 현재 | 현재 |
| 교차 리전 집계 활성화 구성 | 임의 | – | – |
| 홈 리전 및 연결된 리전 선택 | 임의(홈 리전을 변경하려면 중앙 구성을 중지했다가 다시 시작해야 함) | – | – |
| 사용자 지정 작업 구성 | 현재 | 현재 | 현재 |
| 자동화 규칙 구성 | 임의 | – | – |
| 사용자 지정 인사이트 구성 | 현재 | 현재 | 현재 |

Organizations와 통합하고 로컬 구성을 사용하는 경우, 허용되는 작업

Organizations와 통합하고 로컬 구성을 사용하는 경우, 관리자 및 멤버 계정은 다음과 같이 Security Hub CSPM 작업에 액세스할 수 있습니다.

| 작업 | Security Hub CSPM 위임된 관리자 계정 | 멤버 계정 |
| --- | --- | --- |
| Security Hub CSPM 구성 정책 생성 및 관리 | – | – |
| 조직 세부 정보 보기 | 임의 | – |
| 멤버 계정 연결 해지 | 임의 | – |
| 멤버 계정 삭제 | – | – |
| Security Hub CSPM 비활성화 | – | 현재(계정이 위임된 관리자와 연결 해제된 경우) |
| 조사 결과 및 조사 결과 기록 보기 | 임의 | 현재 |
| 조사 결과 업데이트 | 임의 | 현재 |
| 인사이트 결과 보기 | 임의 | 현재 |
| 제어 기능 세부 정보 보기 | 임의 | 현재 |
| 통합 제어 기능에 대한 조사 결과 켜기 또는 끄기 | 임의 | – |
| 표준 활성화 및 비활성화 | 현재 | 현재 |
| 새로운 조직 계정에서 Security Hub CSPM 및 기본 표준을 자동으로 활성화 | 현재 계정 및 새로운 조직 계정의 경우 | – |
| 제어 기능 활성화 및 비활성화 | 현재 | 현재 |
| 통합 활성화 및 비활성화 | 현재 | 현재 |
| 교차 리전 집계 활성화 구성 | 임의 | – |
| 사용자 지정 작업 구성 | 현재 | 현재 |

| 작업 | Security Hub CSPM 위임된 관리자 계정 | 멤버 계정 |
|---|---|---|
| 자동화 규칙 구성 | 임의 | – |
| 사용자 지정 인사이트 구성 | 현재 | 현재 |

초대 기반 계정에 허용된 작업

초대 기반 방법을 사용하여와 통합하는 대신 계정을 수동으로 관리하는 경우 관리자 및 멤버 계정은 다음과 같이 Security Hub CSPM 작업에 액세스할 수 있습니다AWS Organizations.

| 작업 | Security Hub CSPM 관리자 계정 | 멤버 계정 |
|---|---|---|
| Security Hub CSPM 구성 정책 생성 및 관리 | – | – |
| 조직 세부 정보 보기 | 임의 | – |
| 멤버 계정 연결 해지 | 임의 | 현재 |
| 멤버 계정 삭제 | 임의 | – |
| Security Hub CSPM 비활성화 | 현재(활성화된 멤버 계정이 없는 경우) | 현재(계정이 관리자 계정과 연결 해제된 경우) |
| 조사 결과 및 조사 결과 기록 보기 | 임의 | 현재 |
| 조사 결과 업데이트 | 임의 | 현재 |
| 인사이트 결과 보기 | 임의 | 현재 |
| 제어 기능 세부 정보 보기 | 임의 | 현재 |
| 통합 제어 기능에 대한 조사 결과 켜기 또는 끄기 | 임의 | – |

| 작업 | Security Hub CSPM 관리자 계정 | 멤버 계정 |
|---|---|---|
| 표준 활성화 및 비활성화 | 현재 | 현재 |
| 새로운 조직 계정에서 Security Hub CSPM 및 기본 표준을 자동으로 활성화 | – | – |
| 제어 기능 활성화 및 비활성화 | 현재 | 현재 |
| 통합 활성화 및 비활성화 | 현재 | 현재 |
| 교차 리전 집계 활성화 구성 | 임의 | – |
| 사용자 지정 작업 구성 | 현재 | 현재 |
| 자동화 규칙 구성 | 임의 | – |
| 사용자 지정 인사이트 구성 | 현재 | 현재 |

## 계정 작업이 Security Hub CSPM 데이터에 미치는 영향

이러한 계정 작업은 AWSSecurity Hub CSPM 데이터에 다음과 같은 영향을 미칩니다.

### Security Hub CSPM이 비활성화됨

중앙 구성을 사용하는 경우, 위임된 관리자(DA)는 특정 계정 및 조직 단위(OU)에서 AWS Security Hub CSPM을 비활성화하는 Security Hub CSPM 구성 정책을 만들 수 있습니다. 이 경우, 홈 리전 및 연결된 리전의 지정된 계정 및 OU에서 Security Hub CSPM이 비활성화됩니다. 중앙 구성을 사용하지 않는 경우, Security Hub CSPM을 활성화한 각 계정 및 리전에서 개별적으로 Security Hub CSPM을 비활성화해야 합니다. DA 계정에서 Security Hub CSPM이 비활성화된 경우에도 중앙 구성을 사용할 수 없습니다.

관리자 계정에서 Security Hub CSPM이 비활성화된 경우, 관리자 계정에 대한 조사 결과는 생성되거나 업데이트되지 않습니다. 기존 보관된 조사 결과는 30일 후에 삭제됩니다. 기존 활성 조사 결과는 90일 후에 삭제됩니다.

다른 와의 통합이 제거AWS 서비스됩니다.

활성화된 보안 표준 및 제어가 비활성화됩니다.

멤버 계정 연결, 사용자 지정 작업, 인사이트 및 서드 파티 제품 구독을 포함한 기타 Security Hub CSPM 데이터 및 설정은 90일 동안 유지됩니다.

## 구성원 계정이 마스터 계정에서 연결 해제됨

구성원 계정이 마스터 계정으로부터 연결이 해제되면 마스터 계정은 구성원 계정 조사 결과를 볼 수 있는 권한을 잃습니다. 하지만 Security Hub CSPM은 두 계정 모두에서 여전히 활성화됩니다.

중앙 구성을 사용하는 경우, DA는 DA 계정에서 연결 해제된 멤버 계정에 대해 Security Hub CSPM을 구성할 수 없습니다.

관리자 계정에 정의된 사용자 지정 설정 또는 통합은 이전 멤버 계정에서 얻은 결과에 적용되지 않습니다. 예를 들어, 계정 연결이 끊긴 후 Amazon EventBridge 규칙의 이벤트 패턴으로 사용되는 관리자 계정에 사용자 지정 작업이 있을 수 있습니다. 하지만, 멤버 계정에서는 이 사용자 지정 작업을 사용할 수 없습니다.

Security Hub CSPM 관리자 계정의 계정 목록에서 제거된 계정의 상태는 연결 해제됨입니다.

## 멤버 계정이 조직에서 제거

멤버 계정이 조직에서 제거되면 Security Hub CSPM 관리자 계정은 멤버 계정의 조사 결과를 볼 수 있는 권한을 잃게 됩니다. 하지만 Security Hub CSPM은 제거 전과 동일한 설정으로 두 계정 모두에서 계속 활성화됩니다.

중앙 구성을 사용하는 경우, 위임된 관리자가 속한 조직에서 제거된 후에는 멤버 계정에 대해 Security Hub CSPM을 구성할 수 없습니다. 하지만 수동으로 변경하지 않는 한 계정은 제거 이전의 설정을 그대로 유지합니다.

Security Hub CSPM 관리자 계정의 계정 목록에서 제거된 계정의 상태는 삭제됨입니다.

## 계정이 일시 중지되었습니다.

AWS 계정이 일시 중지되면 계정은 Security Hub CSPM에서 결과를 볼 수 있는 권한을 잃게 됩니다. 해당 계정에 대한 조사 결과가 생성되거나 업데이트되지 않습니다. 일시 중지된 계정의 관리자 계정은 계정의 기존 조사 결과를 볼 수 있습니다.

조직 계정의 경우, 멤버 계정 상태가 계정 일시 중단됨으로 변경될 수도 있습니다. 관리자 계정이 계정을 활성화하려고 시도하는 동시에 계정이 일시 중지되면 이런 상황이 발생합니다. 계정 일시 중지됨 계

정의 관리자 계정은 해당 계정의 조사 결과를 볼 수 없습니다. 그 외에는 일시 중지됨 상태는 멤버 계정 상태에 영향을 주지 않습니다.

중앙 구성을 사용하는 경우, 위임된 관리자가 구성 정책을 일시 중지된 계정과 연결하려고 하면 정책 연결이 실패합니다.

90일이 지나면 계정이 해지되거나 다시 활성화됩니다. 계정이 다시 활성화되면 Security Hub CSPM 권한이 복원됩니다. 멤버 계정 상태가 계정 일시 중단됨인 경우, 관리자 계정이 이 계정을 수동으로 활성화해야 합니다.

### 계정이 폐쇄되었습니다.

AWS 계정가 닫히면 Security Hub CSPM은 다음과 같이 해지에 응답합니다.

계정이 Security Hub CSPM 관리자 계정인 경우, 관리자 계정으로서 제거되고 모든 멤버 계정이 제거됩니다. 계정이 멤버 계정인 경우, Security Hub CSPM 관리자 계정에서 연결 해제되고 멤버로서 제거됩니다.

Security Hub CSPM은 기존 보관된 조사 결과를 30일 동안 계정에 유지합니다. 제어 조사 결과의 경우 30일 계산은 조사 결과의 `UpdatedAt` 필드 값을 기준으로 합니다. 다른 유형의 조사 결과의 경우 계산은 조사 결과의 `UpdatedAt` 또는 `ProcessedAt` 필드 값 중 가장 늦은 날짜를 기준으로 합니다. 30일 기간이 종료되는 시점에 Security Hub CSPM은 계정의 모든 조사 결과를 영구적으로 삭제합니다.

Security Hub CSPM은 기존 활성 조사 결과를 90일 동안 계정에 유지합니다. 제어 조사 결과의 경우 90일 계산은 조사 결과의 `UpdatedAt` 필드 값을 기준으로 합니다. 다른 유형의 조사 결과의 경우 계산은 조사 결과의 `UpdatedAt` 또는 `ProcessedAt` 필드 값 중 가장 늦은 날짜를 기준으로 합니다. 90일 기간이 종료되는 시점에 Security Hub CSPM은 계정의 모든 조사 결과를 영구적으로 삭제합니다.

기존 조사 결과를 장기간 유지하려면 조사 결과를 S3 버킷으로 내보낼 수 있습니다. 이 작업은 Amazon EventBridge 규칙과 함께 사용자 지정 작업을 사용하여 수행할 수 있습니다. 자세한 내용은 자동 응답 및 문제 해결을 위해 EventBridge 사용 단원을 참조하십시오.

> **Important**
>
> 의 고객의 경우 AWS GovCloud (US) Regions계정을 해지하기 전에 정책 데이터 및 기타 계정 리소스를 백업한 다음 삭제합니다. 계정을 해지한 후에는 리소스 및 데이터에 액세스할 수 없습니다.

자세한 내용은 AWS Account Management 참조 안내서의 AWS 계정 폐쇄를 참조하세요.

# Security Hub CSPM의 교차 리전 집계 이해

> **Note**
>
> 이제 집계 리전을 홈 리전이라고 합니다. 일부 Security Hub CSPM API 작업은 여전히 이전 용어인 집계 영역을 사용합니다.

AWSSecurity Hub CSPM에서 교차 리전 집계를 사용하면 여러에서 단일 홈 리전으로 조사 결과, 조사 결과 업데이트, 인사이트, 제어 규정 준수 상태 및 보안 점수를 집계AWS 리전할 수 있습니다. 그러면 홈 리전으로부터 이 모든 데이터를 관리할 수 있습니다.

미국 동부(버지니아 북부)를 홈 리전으로 설정하고 미국 서부(오리건) 및 미국 서부(캘리포니아 북부)를 연결 리전으로 설정한다고 가정해 보겠습니다. 미국 동부(버지니아 북부)의 조사 결과 페이지를 보면 세 리전 모두의 조사 결과를 볼 수 있습니다. 이러한 조사 결과에 대한 업데이트도 세 리전 모두에 반영됩니다.

> **Note**
>
> 에서 AWS GovCloud (US)교차 리전 집계는 조사 결과, 조사 결과 업데이트 및 인사이트에 대해서만 지원됩니다AWS GovCloud (US). 특히 AWSGovCloud(미국 동부)와 AWSGovCloud(미국 서부) 간에 조사 결과, 조사 결과 업데이트 및 인사이트만 집계할 수 있습니다. 중국 리전에서는 중국 리전 전반의 조사 결과, 조사 결과 업데이트 및 인사이트에 대해서만 교차 리전 집계 활성화가 지원됩니다. 특히 중국(베이징) 및 중국(닝샤) 간에는 조사 결과, 조사 결과 업데이트, 인사이트만 집계할 수 있습니다.

연결된 리전에서는 제어가 활성화되었지만 홈 리전에서는 비활성화된 경우, 홈 리전에서 제어의 규정 준수 상태를 볼 수 있지만 홈 리전에서는 해당 제어를 활성화하거나 비활성화할 수 없습니다. 중앙 구성을 사용하는 경우는 예외입니다. 중앙 구성을 사용하는 경우, 위임된 Security Hub CSPM 관리자는 홈 리전에서 제어를 구성하고 홈 리전에서 연결된 리전을 구성할 수 있습니다.

홈 리전을 설정한 경우, 보안 점수는 모든 연결된 리전의 제어 상태를 설명합니다. 리전 간 보안 점수 및 규정 준수 상태를 보려면 Security Hub CSPM을 사용하는 IAM 역할에 다음 권한을 추가하세요.

- `ListSecurityControlDefinitions`
- `BatchGetStandardsControlAssociations`

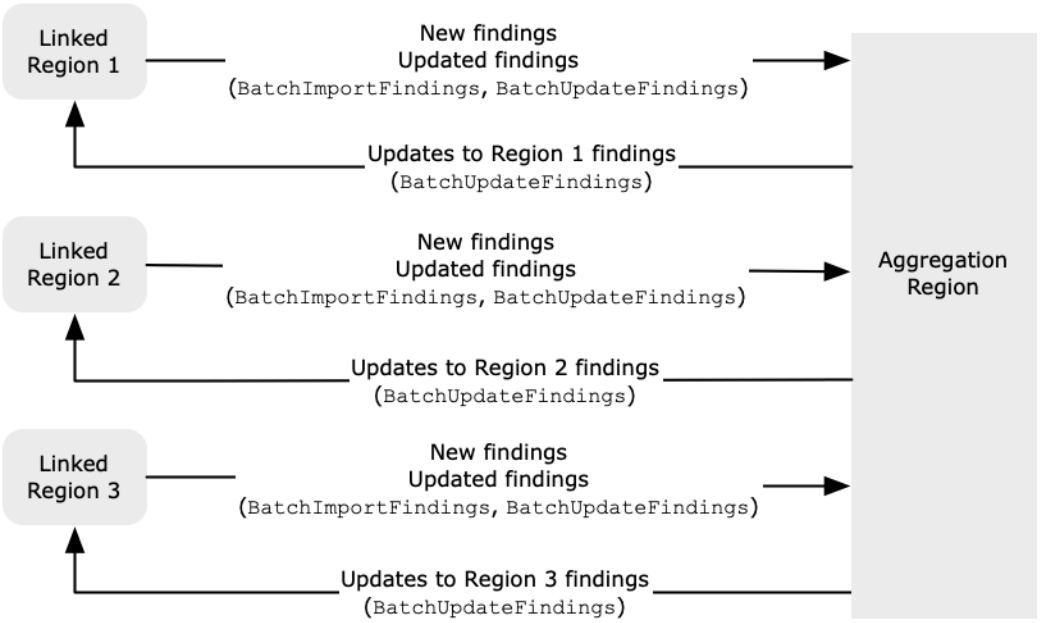
- BatchUpdateStandardsControlAssociations

## 집계되는 데이터 유형

교차 리전 집계가 하나 이상의 연결된 리전으로 활성화되면 Security Hub CSPM은 연결된 리전에서 홈 리전으로 다음 데이터를 복제합니다. 이는 교차 리전 집계가 활성화된 모든 계정에서 발생합니다.

- 조사 결과
- 인사이트
- 제어 규정 준수 상태
- 보안 점수

이전 목록의 새로운 데이터 외에 Security Hub CSPM은 연결된 리전과 홈 리전 간에 이 데이터에 대한 업데이트를 복제합니다. 연결된 리전에서 발생한 업데이트는 홈 리전에 복제됩니다. 홈 리전에서 발생한 업데이트는 연결된 리전으로 다시 복제됩니다. 집계 영역과 연결 리전의 업데이트가 충돌하는 경우, 가장 최근 업데이트가 사용됩니다.




교차 리전 집계는 Security Hub CSPM 비용에 추가되지 않습니다. Security Hub CSPM에서 새로운 데이터나 업데이트를 복제할 때는 요금이 부과되지 않습니다.

홈 리전의 요약 페이지에서는 연결된 리전 전반에 활성화된 조사 결과를 볼 수 있습니다. 자세한 내용은 심각도별 조사 결과에 대한 교차 리전 요약 보기를 참조하세요. 조사 결과를 분석하는 기타 요약 페이지 패널에는 연결된 리전 전반의 정보도 표시됩니다.

홈 리전의 보안 점수는 전달된 제어의 수를 연결된 모든 리전에서 활성화된 제어의 수와 비교하여 계산됩니다. 또한 하나 이상의 연결된 리전에서 제어가 활성화된 경우, 홈 리전의 보안 표준 세부 정보 페이지에서 해당 제어를 볼 수 있습니다. 표준 세부 정보 페이지의 규제 준수 상태는 연결 리전 전반의 조사 결과를 반영합니다. 하나 이상의 연결된 리전에서 제어와 관련된 보안 검사에 실패하는 경우, 홈 리전의 표준 세부 정보 페이지에 해당 제어의 규정 준수 상태가 실패로 표시됩니다. 보안 검사 수에는 연결된 모든 리전의 조사 결과가 포함됩니다.

Security Hub CSPM은 계정에 Security Hub CSPM이 활성화된 리전의 데이터만 집계합니다. Security Hub CSPM은 교차 리전 집계 구성을 기반으로 하는 계정에 대해 자동으로 활성화되지 않습니다.

연결된 리전을 선택하지 않고 교차 리전 집계를 활성화할 수 있습니다. 이 경우, 데이터 복제가 발생하지 않습니다.

## 관리자 및 멤버 계정의 집계

독립형 계정, 멤버 계정 및 관리자 계정은 교차 리전 집계를 구성할 수 있습니다. 관리자가 구성한 경우, 관리형 계정에서 교차 리전 집계가 작동하려면 관리자 계정이 꼭 있어야 합니다. 멤버 계정이 관리자 계정에서 제거되거나 연결 해제되면 해당 멤버 계정에 대한 교차 리전 집계가 중지됩니다. 이는 관리자와 멤버 관계가 시작되기 전에 해당 계정에 교차 리전 집계가 활성화된 경우에도 마찬가지입니다.

관리자 계정이 교차 리전 집계를 활성화하면 Security Hub CSPM은 관리자 계정이 모든 연결된 리전에서 생성하는 데이터를 홈 리전에 복제합니다. 또한 Security Hub CSPM은 해당 관리자와 연결된 멤버 계정을 식별하고 각 멤버 계정은 관리자의 교차 리전 집계 설정을 상속합니다. Security Hub CSPM은 멤버 계정이 모든 연결된 리전에서 생성하는 데이터를 홈 리전에 복제합니다.

관리자는 관리되는 리전 내의 모든 멤버 계정에서 보안 조사 결과에 액세스하고 관리할 수 있습니다. 그러나 Security Hub CSPM 관리자는 홈 리전에 로그인하여 모든 멤버 계정 및 연결된 리전의 집계된 데이터를 확인해야 합니다.

Security Hub CSPM 멤버 계정으로 홈 리전에 로그인해야 모든 연결된 리전의 계정에서 집계된 데이터를 볼 수 있습니다. 멤버 계정에는 다른 멤버 계정의 데이터를 볼 수 있는 권한이 없습니다.

관리자 계정은 멤버 계정을 수동으로 초대하거나와 통합된 조직의 위임된 관리자 역할을 할 수 있습니다AWS Organizations. 수동으로 초대된 멤버 계정의 경우, 교차 리전 집계가 작동하려면 관리자가 홈 리전 및 연결된 모든 리전에서 계정을 초대해야 합니다. 또한 관리자가 멤버 계정의 조사 결과를 볼 수 있도록 멤버 계정은 홈 리전 및 모든 연결된 리전에서 Security Hub CSPM이 활성화되어 있어야 합니다. 홈 리전을 다른 목적으로 사용하지 않는 경우, 해당 리전에서 Security Hub CSPM 표준 및 통합을 비활성화하여 요금을 방지할 수 있습니다.

교차 리전 집계 사용할 계획이고 관리자 계정이 여러 개 있는 경우, 다음과 같은 모범 사례를 권장합니다.

- 각 관리자 계정에는 서로 다른 구성원 계정이 있습니다.
- 각 관리자 계정은 여러 리전에서 동일한 구성원 계정을 가집니다.
- 각 관리자 계정은 서로 다른 홈 리전을 사용합니다.

> **Note**
>
> 이 교차 리전 집계이 중앙 구성에 미치는 영향을 이해하려면 중앙 구성이 교차 리전 집계에 미치는 영향 섹션을 참조하세요.

## 중앙 구성이 교차 리전 집계에 미치는 영향

중앙 구성은 통합 시 사용할 수 있는 AWSSecurity Hub CSPM의 옵트인 기능입니다AWS Organizations. 중앙 구성을 사용하는 경우, 위임된 관리자 계정으로 조직의 계정 및 조직 단위(OU)에 대한 Security Hub CSPM 서비스, 표준 및 제어를 구성할 수 있습니다. 계정 및 OU를 구성하기 위해 위임된 관리자는 Security Hub CSPM 구성 정책을 생성합니다. 구성 정책을 사용하여 Security Hub CSPM의 활성화 또는 비활성화 여부와 활성화되는 표준 및 제어를 정의할 수 있습니다. 위임된 관리자는 구성 정책을 특정 계정, OU 또는 루트(전체 조직)와 연결합니다.

위임된 관리자는 홈 리전에서만 조직에 대한 구성 정책을 만들고 관리할 수 있습니다. 또한 구성 정책은 홈 리전 및 연결된 모든 리전에 적용됩니다. 일부 연결된 리전에만 적용되고 다른 리전에는 적용되지 않는 구성 정책을 만들 수 없습니다. 교차 리전 집계 활성화에 대한 자세한 내용은 교차 리전 집계 활성화를 참조하세요.

중앙 구성을 사용하려면 홈 리전을 지정해야 합니다. 선택 사항으로, 하나 이상의 리전을 연결된 리전으로 선택할 수 있습니다. 또한 연결된 리전 없이 홈 리전을 지정하도록 선택할 수도 있습니다.

교차 리전 집계 활성화 설정을 변경하면 구성 정책에 영향을 미칠 수 있습니다. 연결된 리전을 추가하면 구성 정책이 해당 리전에 적용됩니다. 리전이 옵트인 리전인 경우, 해당 리전에 구성 정책이 적용되려면 해당 리전을 활성화해야 합니다. 반대로 연결된 리전을 제거하면 해당 리전에는 구성 정책이 더 이상 적용되지 않습니다. 해당 리전의 계정은 연결된 리전이 제거되었을 때의 설정을 유지합니다. 이러한 설정을 변경할 수 있지만 각 계정 및 리전에서 개별적으로 변경해야 합니다.

홈 리전을 제거하거나 변경하면 구성 정책 및 정책 연결이 삭제됩니다. 더 이상 어떤 리전에서도 중앙 구성을 사용하거나 구성 정책을 만들 수 없습니다. 계정은 홈 리전이 변경되거나 제거되기 전의 설정을

유지합니다. 이러한 설정은 언제든지 변경할 수 있지만 더 이상 중앙 구성을 사용하지 않으므로 각 계정 및 리전에서 설정을 개별적으로 수정해야 합니다. 새로운 홈 리전을 지정하는 경우, 중앙 구성을 사용하고 구성 정책을 다시 만들 수 있습니다.

중앙 구성에 대한 자세한 내용은 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

## 교차 리전 집계 활성화 활성화하기

> **Note**
>
> 이제 집계 리전을 홈 리전이라고 합니다. 일부 Security Hub CSPM API 작업은 여전히 이전 용어인 집계 영역을 사용합니다.

홈 리전으로 지정AWS 리전하려는에서 교차 리전 집계를 활성화해야 합니다.

교차 리전 집계를 활성화하려면 조사 결과 집계자라는 Security Hub CSPM 리소스를 생성합니다. 조사 결과 집계자 리소스는 홈 리전 및 연결된 리전(있는 경우)을 지정합니다.

기본적으로 비활성화AWS 리전된는 홈 리전으로 사용할 수 없습니다. 기본적으로 비활성화되는 리전 목록은 AWS 일반 참조에서 리전 활성화를 참조하세요.

교차 리전 집계를 활성화할 때 원하는 경우, 하나 이상의 연결된 리전을 지정하도록 선택할 수 있습니다. 또한 Security Hub CSPM에서 새로운 리전을 지원하기 시작하고 선택한 경우, 새로운 리전을 자동으로 연결할지 여부도 선택할 수 있습니다.

Security Hub CSPM console

교차 리전 집계 활성화를 활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. AWS 리전선택기를 사용하여 집계 리전으로 사용할 리전에 로그인합니다.
3. Security Hub CSPM 탐색 메뉴에서 설정을 선택한 다음 리전을 선택합니다.
4. 조사 결과 집계에서 조사 결과 집계 구성을 선택합니다.

   기본적으로, 홈 리전은 집계 리전 없음으로 설정됩니다.
5. 집계 리전에서 옵션을 선택하여 현재 리전을 홈 리전으로 지정하는 옵션을 선택합니다.
6. 필요에 따라 연결된 리전에서 데이터를 집계할 리전을 선택합니다.

7. Security Hub CSPM에서 지원하므로 파티션에 있는 새로운 리전의 데이터를 자동으로 집계하고 사용자가 이를 선택하도록 하려면 미래 리전 연결을 선택합니다.
8. 저장을 선택합니다.

### Security Hub CSPM API

홈 리전으로 사용하기 원하는 리전에서 Security Hub CSPM API의 `CreateFindingAggregator` 작업을 사용합니다. 를 사용하는 경우 create-finding-aggregator 명령을 AWS CLI실행합니다.

`RegionLinkingMode`에서 다음 옵션 중 하나를 선택합니다.

- `ALL_REGIONS` - Security Hub CSPM은 모든 리전의 데이터를 집계합니다. 또한 Security Hub CSPM은 새로운 리전이 지원되고 사용자가 이를 선택할 때 해당 리전의 데이터도 집계합니다.
- `ALL_REGIONS_EXCEPT_SPECIFIED` - Security Hub CSPM은 사용자가 제외하려는 리전을 제외한 모든 리전의 데이터를 집계합니다. 또한 Security Hub CSPM은 새로운 리전이 지원되고 사용자가 이를 선택할 때 해당 리전의 데이터도 집계합니다. 집계에서 제외할 리전 목록을 제공하는 데 `Regions`을(를) 사용합니다.
- `SPECIFIED_REGIONS`- Security Hub CSPM은 선택된 리전 목록에서 데이터를 집계합니다. Security Hub CSPM은 자동으로 새로운 리전의 데이터를 집계하지 않습니다. 집계할 리전 목록을 제공하는 데 `Regions`을(를) 사용합니다.
- `NO_REGIONS` - 연결된 리전을 선택하지 않았으므로 Security Hub CSPM은 데이터를 집계하지 않습니다.

다음 예제에서는 교차 리전 집계가 구성되어 있습니다. 해당 홈 리전은 미국 동부(버지니아 북부)입니다. 연결된 리전은 미국 서부(캘리포니아 북부) 및 미국 서부(오레곤)입니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub create-finding-aggregator --region us-east-1 --region-linking-
mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

# 교차 리전 집계 설정 검토

> **Note**
>
> 이제 집계 리전을 홈 리전이라고 합니다. 일부 Security Hub CSPM API 작업은 여전히 이전 용어인 집계 영역을 사용합니다.

모든에서 AWSSecurity Hub CSPM의 현재 리전 간 집계 구성을 볼 수 있습니다AWS 리전. 구성에는 홈 리전, 연결된 리전(있는 경우) 및 Security Hub CSPM이 지원하는 새로운 리전을 자동으로 연결할지 여부가 포함됩니다.

멤버 계정에서 관리자 계정이 구성한 교차 리전 집계 설정도 볼 수 있습니다.

원하는 방법을 선택하고 단계에 따라 현재 교차 리전 집계 설정을 확인합니다.

Security Hub CSPM console

교차 리전 집계 설정을 보려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 리전 탭을 선택합니다.

교차 리전 집계 활성화가 활성화되지 않은 경우, 리전 탭에 교차 리전 집계 활성화를 활성화하는 옵션이 표시됩니다. 관리자 계정 및 독립 실행형 계정만 교차 리전 집계 활성화를 활성화할 수 있습니다.

교차 리전 집계 활성화가 활성화된 경우, 리전 탭에 다음 정보가 표시됩니다.

- 홈 리전
- Security Hub CSPM이 지원하고 사용자가 선택한 새로운 리전의 조사 결과, 인사이트, 제어 상태 및 보안 점수를 자동으로 집계할지 여부
- 연결된 리전 목록(선택한 경우)

Security Hub CSPM API

교차 리전 집계 설정을 검토하려면(Security Hub CSPM API)

Security Hub CSPM API의 `GetFindingAggregator` 작업을 사용합니다. 를 사용하는 경우 get-finding-aggregator 명령을 AWS CLI실행합니다.

요청을 할 때 조사 결과 집계 ARN을 제공해야 합니다. 조사 결과 집계자 ARN을 가져오려면 `ListFindingAggregators` 작업 또는 list-finding-aggregators 명령을 사용합니다.

다음 예제에서는 지정된 조사 결과 집계자 ARN에 대한 교차 리전 집계 설정을 보여줍니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$aws securityhub get-finding-aggregator --finding-aggregator-
arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-
e89b-12d3-a456-426652340000
```

## 교차 리전 집계 설정 업데이트

> **Note**
>
> 이제 집계 리전을 홈 리전이라고 합니다. 일부 Security Hub CSPM API 작업은 여전히 이전 용어인 집계 영역을 사용합니다.

연결된 리전 또는 현재 홈 리전을 변경하여 AWSSecurity Hub CSPM에서 현재 리전 간 집계 설정을 업데이트할 수 있습니다. AWS 리전Security Hub CSPM이 지원되는 새의 데이터를 자동으로 집계할지 여부도 변경할 수 있습니다.

교차 리전 집계에 대한 변경 사항은 AWS 계정에서 해당 리전이 활성화될 때까지 옵트인 리전에 대해 구현되지 않습니다. 2019년 3월 20일 이후에 AWS도입된 리전은 옵트인 리전입니다.

연결된 리전에서 데이터 집계를 중지하면AWSSecurity Hub CSPM은 홈 리전에서 액세스할 수 있는 해당 리전에서 기존 집계된 데이터를 제거하지 않습니다.

이 섹션의 업데이트 절차를 사용하여 홈 리전을 변경할 수 없습니다. 홈 리전을 변경하려면 다음을 수행해야 합니다.

1. 교차 리전 집계 활성화 중지 지침은 the section called “집계 중지” 섹션을 참조하세요.
2. 새로운 홈 리전으로 설정하려는 리전으로 변경합니다.
3. 교차 리전 집계 활성화를 활성화 지침은 the section called “집계 활성화” 섹션을 참조하세요.

현재 홈 리전에서 교차 리전 집계 구성을 업데이트해야 합니다.

Security Hub CSPM console

연결된 리전을 변경하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

   현재 집계 전으로 로그인합니다.
2. Security Hub CSPM 탐색 메뉴에서 설정을 선택한 다음 리전을 선택합니다.
3. 조사 결과 집계에서 편집을 선택합니다.
4. 연결된 리전의 경우, 선택한 연결된 리전을 업데이트합니다.
5. 필요한 경우, 미래 리전 연결 선택 여부를 변경합니다. 이 설정은 Security Hub CSPM이 새로운 리전에 대한 지원을 추가하고 사용자가 선택할 때 새로운 리전을 자동으로 연결할지 여부를 결정합니다.
6. 저장을 선택합니다.

Security Hub CSPM API

`UpdateFindingAggregator` 작업을 사용합니다. 를 사용하는 경우 update-finding-aggregator 명령을 AWS CLI실행합니다. 조사 결과 집계자를 식별하려면 조사 결과 집계자 ARN을 제공해야 합니다. 조사 결과 집계자 ARN을 가져오려면 `ListFindingAggregators` 작업 또는 list-finding-aggregators 명령을 사용합니다.

연결 모드가 `ALL_REGIONS_EXCEPT_SPECIFIED`또는 `SPECIFIED_REGIONS`인 경우, 제외된 또는 포함된 리전 목록을 변경할 수 있습니다. 리전 연결 모드를 `NO_REGIONS`로 변경하려면 리전 목록을 제공해서는 안 됩니다.

제외 또는 포함된 리전 목록을 변경할 때는 업데이트와 함께 전체 목록을 제공해야 합니다. 예를 들어, 현재 미국 동부(오하이오) 의 조사 결과를 집계하고 있고 미국 서부(오레곤) 의 조사 결과도 집계하려는 경우를 가정해 보겠습니다. 미국 동부(오하이오)와 미국 서부(오리건)을 모두 포함하는 `Regions` 목록을 제공해야 합니다.

다음 예제에서는 교차 리전 집계를 선택한 리전에 업데이트합니다. 이 명령은 현재 홈 리전인 미국 동부(버지니아 북부)에서 실행됩니다. 연결된 리전은 미국 서부(캘리포니아 북부) 및 미국 서부(오레곤)입니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
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
```

## 교차 리전 집계 활성화 중지

> **Note**
>
> 이제 집계 리전을 홈 리전이라고 합니다. 일부 Security Hub CSPM API 작업은 여전히 이전 용어인 집계 영역을 사용합니다.

AWSSecurity Hub CSPM이 데이터를 집계하지 않도록 하려면 결과 집계자를 삭제할 수 있습니다. 또는 기존 애그리게이터AWS 리전를 연결 모드로 업데이트하여 결과 애그리게이터를 유지하고 홈 리전에 NO_REGIONS 연결할 수 없습니다.

홈 리전을 변경하려면 현재 조사 결과 집계자를 삭제하고 새로운 집계자를 생성해야 합니다.

조사 결과 집계자를 삭제하면 Security Hub CSPM이 데이터 집계를 중지합니다. 이는 홈 리전에서 기존 집계 데이터는 제거되지 않습니다.

### 조사 결과 집계자 삭제(콘솔)

현재 홈 리전에서만 조사 결과 집계자를 삭제할 수 있습니다.

홈 리전이 아닌 리전의 경우, Security Hub CSPM 콘솔의 조사 결과 집계 패널에는 홈 리전의 구성을 편집해야 한다는 메시지가 표시됩니다. 이 메시지를 선택하면 홈 리전으로 전환할 수 있는 링크가 표시됩니다.

Security Hub CSPM console

교차 리전 집계를 중지하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 홈 리전에 로그인했는지 확인합니다.
3. Security Hub CSPM 탐색 메뉴에서 설정을 선택한 다음 리전을 선택합니다.
4. 조사 결과 집계에서 편집을 선택합니다.

5. 집계 영역에서 집계 영역 없음을 선택합니다.
6. 저장을 선택합니다.
7. 확인 필드의 확인 대화 상자에 **Confirm**을 입력합니다.
8. 확인을 선택합니다.

Security Hub CSPM API

Security Hub CSPM API의 DeleteFindingAggregator 작업을 사용합니다. 를 사용하는 경우 delete-finding-aggregator 명령을 AWS CLI실행합니다.

삭제할 조사 결과 집계자를 식별하려면 조사 결과 집계자 ARN을 제공합니다. 조사 결과 집계자 ARN을 가져오려면 ListFindingAggregators 작업 또는 list-finding-aggregators 명령을 사용합니다.

다음 예제에서는 조사 결과 집계자를 삭제합니다. 이 명령은 현재 홈 리전인 미국 동부(버지니아 북부)에서 실행됩니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$aws securityhub delete-finding-aggregator arn:aws:securityhub:us-
east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --
region us-east-1
```

# Security Hub CSPM의 보안 표준 이해

AWS Security Hub CSPM에서 보안 표준은 규제 프레임워크, 업계 모범 사례 또는 회사 정책을 기반으로 하는 일련의 요구 사항입니다. 각 표준에 적용되는 보안 제어를 포함하여 Security Hub CSPM이 현재 지원하는 표준에 대한 자세한 내용은 Security Hub CSPM용 표준 참조 섹션을 참조하세요.

표준을 활성화하면 Security Hub CSPM은 표준에 적용되는 모든 제어를 자동으로 활성화합니다. 그런 다음 Security Hub CSPM은 제어에 대한 보안 검사를 실행하여 Security Hub CSPM 조사 결과를 생성합니다. 필요에 따라 개별 제어를 비활성화하고 나중에 다시 활성화할 수 있습니다. 표준을 완전히 비활성화할 수도 있습니다. 표준을 비활성화하면 Security Hub CSPM은 해당 표준에 적용되는 제어에 대한 보안 검사 실행을 중지합니다. 해당 제어에 대한 조사 결과는 더 이상 생성되지 않습니다.

조사 결과 외에도 Security Hub CSPM은 활성화하는 각 표준에 대한 보안 점수를 생성합니다. 점수는 표준에 적용되는 제어의 상태를 기반으로 합니다. 집계 영역을 설정한 경우 표준의 보안 점수는 모든

연결된 리전의 제어 상태를 반영합니다. 조직의 Security Hub CSPM 관리자인 경우 점수에는 조직 내 모든 계정의 제어 상태가 반영됩니다. 자세한 내용은 보안 점수 계산 단원을 참조하십시오.

표준을 검토하고 관리하려면 Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용할 수 있습니다. 콘솔의 보안 표준 페이지에는 Security Hub CSPM이 현재 지원하는 보안 표준이 나열됩니다. 여기에는 각 표준에 대한 설명과 표준의 현재 상태가 포함됩니다. 또한 표준을 활성화하면 이 페이지를 사용하여 표준에 대한 추가 세부 정보에 액세스할 수 있습니다. 예를 들어 다음 정보를 검토할 수 있습니다.

- 표준의 현재 보안 점수.
- 표준에 적용되는 제어에 대한 집계 통계.
- 각 표준의 규정 준수 상태를 포함하여 표준에 적용되고 현재 활성화되어 있는 제어의 목록.
- 표준에 적용되지만 현재 비활성화된 제어의 목록.

심층 분석을 위해, 데이터를 필터링 및 정렬하고 드릴다운하여 표준에 적용되는 개별 제어의 세부 정보를 검토할 수 있습니다.

단일 계정 및에 대해 개별적으로 표준을 활성화할 수 있습니다 AWS 리전. 그러나 다중 계정 및 다중 리전 환경에서 시간을 절약하고 구성 드리프트를 줄이려면 중앙 구성을 사용하여 표준을 활성화하고 관리하는 것이 좋습니다. 중앙 구성을 사용하면 위임된 Security Hub CSPM 관리자가 여러 계정 및 리전에서 표준을 구성하는 방법을 지정하는 정책을 생성할 수 있습니다.

주제

- Security Hub CSPM용 표준 참조
- 보안 표준 활성화
- 보안 표준 세부 정보 검토
- 자동으로 활성화되는 보안 표준 끄기
- 보안 표준 비활성화

## Security Hub CSPM용 표준 참조

AWS Security Hub CSPM에서 보안 표준은 규제 프레임워크, 업계 모범 사례 또는 회사 정책을 기반으로 하는 일련의 요구 사항입니다. Security Hub CSPM은 이러한 요구 사항을 제어에 매핑하고 제어에 대한 보안 검사를 실행하여 표준 요구 사항이 충족되고 있는지 평가합니다. 각 표준에는 여러 개의 제어가 포함됩니다.

Security Hub CSPM은 현재 다음 표준을 지원합니다.

- AWS 기본 보안 모범 사례 - AWS 및 업계 전문가가 개발한이 표준은 섹터 또는 규모에 관계없이 조직의 보안 모범 사례를 컴파일한 것입니다. 및 AWS 계정 리소스가 보안 모범 사례에서 벗어나는 시점을 감지하는 제어 세트를 제공합니다. 또한 보안 태세를 개선 및 유지하는 방법에 대한 규범적 지침을 제공합니다.
- AI 보안 모범 사례 - AWS 보안 전문가가 개발한이 표준은 배포된 AI 리소스가 보안 모범 사례와 일치하지 않는 경우를 감지하는 엄선된 제어 세트를 제공합니다. 이를 통해 네트워크 격리, 암호화, VPC 배치 및 AWS KMS 키 사용과 같은 도메인을 포함하여 AI 워크로드가 권장 보안 구성에서 벗어나는 영역을 식별할 수 있습니다.
- AWS 리소스 태그 지정 - Security Hub CSPM에서 개발한이 표준을 통해 AWS 리소스에 태그가 있는지 확인할 수 있습니다. 태그는 AWS 리소스의 메타데이터 역할을 하는 키-값 페어입니다. 태그를 사용하면 AWS 리소스를 식별, 분류, 관리 및 검색할 수 있습니다. 예를 들어, 태그를 사용하여 용도, 소유자 또는 환경 기준으로 리소스를 범주화할 수 있습니다.
- CIS AWS 파운데이션 벤치마크 - 인터넷 보안 센터(CIS)에서 개발한이 표준은에 대한 보안 구성 지침을 제공합니다 AWS. 기본, 테스트 가능 및 아키텍처에 구애받지 않는 설정을 중심으로 AWS 서비스 및 리소스의 하위 집합에 대한 보안 구성 지침 및 모범 사례 세트를 지정합니다. 지침에는 명확한 단계별 구현 및 평가 절차가 포함됩니다.
- NIST SP 800-53 개정 5 - 이 표준은 정보 시스템 및 중요 리소스의 기밀성, 무결성, 가용성을 보호하기 위한 NIST(국립 표준 기술 연구소) 요구 사항에 부합합니다. 관련 프레임워크는 일반적으로 미국 연방 기관 또는 정보 시스템과 협력하는 조직에 적용됩니다. 그러나 민간 조직도 이 요구 사항을 지침 프레임워크로 사용할 수 있습니다.
- NIST SP 800-171 개정 2 - 이 표준은 미국 연방 정부에 속하지 않는 시스템 및 조직에서 통제된 미분류 정보(CUI)의 기밀성을 보호하기 위한 NIST 보안 권장 사항 및 요구 사항에 부합합니다. CUI는 연방 정부의 분류 기준을 충족하지 않지만 민감한 정보로 간주되며 미국 연방 정부 또는 미국 연방 정부를 대신하여 기타 기관이 생성 또는 소유하는 정보입니다.
- PCI DSS - 이 표준은 PCI SSC(보안 표준 위원회)에서 정의한 PCI DSS(지불 카드 산업 데이터 보안 표준) 규정 준수 프레임워크에 부합합니다. 이 프레임워크는 신용카드 및 직불카드 정보를 안전하게 처리하기 위한 일련의 규칙 및 지침을 제공하며, 일반적으로 카드 소지자 데이터를 저장, 처리 또는 전송하는 조직에 적용됩니다.
- 서비스 관리형 표준 - AWS Control Tower이 표준은 Security Hub CSPM에서 제공하는 탐지 제어를 구성하는 데 도움이 됩니다 AWS Control Tower.는 규범적 모범 사례에 따라 AWS 다중 계정 환경을 설정하고 관리하는 간단한 방법을 AWS Control Tower 제공합니다.

Security Hub CSPM 표준 및 제어는 규제 프레임워크 또는 감사 준수를 보장하지 않습니다. 대신, AWS 계정 및 리소스의 상태를 평가하고 모니터링하는 방법을 제공합니다. 비즈니스 요구 사항, 산업 또는 사용 사례와 관련된 각 표준을 활성화하는 것을 권장합니다.

개별 제어는 둘 이상의 표준에 적용될 수 있습니다. 여러 표준을 활성화하는 경우 통합 제어 조사 결과도 활성화하는 것이 좋습니다. 이렇게 하면 Security Hub CSPM은 제어가 복수의 표준에 적용되더라도 각 제어에 대해 단일 조사 결과를 생성합니다. 통합 제어 조사 결과를 활성화하지 않으면 Security Hub CSPM은 제어가 적용되는 활성화된 표준에 대해 각각 조사 결과를 생성합니다. 예를 들어 2개의 표준을 활성화하고 두 표준 모두에 제어가 적용되는 경우 각 표준에 대해 하나씩 2개의 개별 제어 조사 결과를 수신하게 됩니다. 통합 제어 조사 결과를 활성화하면 해당 제어에 대해 하나의 조사 결과만 수신됩니다. 자세한 내용은 통합 제어 조사 결과 단원을 참조하십시오.

표준별 세부 참조

- AWS Security Hub CSPM의 기본 보안 모범 사례 표준
- Security Hub CSPM의 AI 보안 모범 사례 표준
- AWS Security Hub CSPM의 리소스 태그 지정 표준
- Security Hub CSPM의 CIS AWS 파운데이션 벤치마크
- Security Hub CSPM의 NIST SP 800-53 개정 5
- Security Hub CSPM의 NIST SP 800-171 개정 2
- Security Hub CSPM의 PCI DSS
- Security Hub CSPM의 서비스 관리형 표준

## AWS Security Hub CSPM의 기본 보안 모범 사례 표준

AWS 및 업계 전문가가 개발한 AWS FSBP(기본 보안 모범 사례) 표준은 조직 부문 또는 규모에 관계없이 조직의 보안 모범 사례를 컴파일한 것입니다. 및 AWS 계정 리소스가 보안 모범 사례에서 벗어나는 시기를 감지하는 제어 세트를 제공합니다. 또한 조직의 보안 태세를 개선 및 유지하는 방법에 대한 규범적 지침을 제공합니다.

AWS Security Hub CSPM의 AWS 기본 보안 모범 사례 표준에는 AWS 계정 및 워크로드를 지속적으로 평가하고 보안 모범 사례에서 벗어나는 영역을 식별하는 데 도움이 되는 제어가 포함되어 있습니다. 제어에는 여러 AWS 서비스(으)로부터의 리소스에 대한 보안 모범 사례가 포함됩니다. 각 제어에는 제어가 적용되는 보안 기능을 반영하는 범주가 할당됩니다. 범주 목록 및 추가 세부 정보는 제어 범주 섹션을 참조하세요.

표준에 적용되는 제어

다음 목록은 기본 AWS 보안 모범 사례 표준(v1.0.0)에 AWS 적용되는 Security Hub CSPM 제어를 지정합니다. 제어의 세부 정보를 검토하려면 해당 제어를 선택하세요.

[Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정

[ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.

[ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.

[APIGateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.

[APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.

[APIGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.

[APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

[APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.

[APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.

[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.

[APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.

[APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.

[AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.

[AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.

[AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.

[AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.

[Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.

[PCI.AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

[AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.

[AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.

[Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.

[AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.

[오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.

[Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.

[BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.

[BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.

[BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.

[BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.

[CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.

[CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.

[CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.

[CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.

[CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.

[CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

[CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.

[CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

[CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.

[CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.

[CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

[CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

[CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.

[CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다

[CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다

[CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.

[CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다.

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.

[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.

[CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.

[CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.

[Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다

[Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다

[Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.

[Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.

[Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.

[Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.

[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.

[DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.

[DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

[DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.

[DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다

[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.

[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.

[DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.

[DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다

[DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.

[DynamoDB.2] DynamoDB 테이블에는 시점 복구가 활성화되어 있어야 합니다.

[DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.

[DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다

[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원 가능하도록 구성해서는 안 됩니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.

[EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.

[EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.

[EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

[EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.

[EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.

[EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.

[EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.

[EC2.20] a AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.

[EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

[EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다

[EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다

[EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다

[EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다

[EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다

[EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.

[EC2.172] EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다

[EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다

[EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다

[EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다

[EC2.182] Amazon EBS 스냅샷에 대해 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

[EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.

[ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.

[ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.

[ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.

[ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.

[ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.

[ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.

[ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.

[ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.

[ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.

[ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.

[ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.

[ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

[ECS.18] ECS 작업 정의는 EFS 볼륨에 대해 전송 중 암호화를 사용해야 합니다.

[ECS.19] ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다.

[ECS.20] ECS 작업 정의는 Linux 컨테이너 정의에서 루트가 아닌 사용자를 구성해야 합니다.

[ECS.21] ECS 작업 정의는 Windows 컨테이너 정의에서 관리자가 아닌 사용자를 구성해야 합니다.

[EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS

[EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.

[EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.

[EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.

[EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.

[EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.

[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.

[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.

[EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.

[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.

[ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

[ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다

[ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.

[ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.

[ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.

[ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.

[ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.

[ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.

[ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.

[ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.

[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

[ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager

[ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.

[ELB.4] Application Load Balancer는 잘못된 http 헤더를 삭제하도록 구성되어야 합니다.

[ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.

[ELB.6] 애플리케이션, 게이트웨이, Network Load Balancers에는 삭제 보호가 활성화되어 있어야 합니다.

[ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.

[ELB.8] SSL AWS Config리스너가 있는 Classic Load Balancer는 강력한 요구 사항이 있는 사전 정의된 보안 정책을 사용해야 합니다.

[ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.

[ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.

[ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.

[ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.

[ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.

[ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다

[ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다

[ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.

[ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.

[EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

[EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다

[EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다

[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

[ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.

[ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.

[ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.

[ES.8] Elasticsearch 도메인에 대한 연결은 TLS 보안 정책을 사용하여 암호화해야 합니다.

[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.

[FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.

[FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.

[FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.

[FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다

[FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다

[Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.

[Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue

[GuardDuty.1] GuardDuty를 활성화해야 합니다.

[GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.

[GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.

[GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.

[GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.

[GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.

[GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.

[GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다

[GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다

[GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.

[Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.

[Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.

[Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.

[Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.

[Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.

[Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.

[KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.

[KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

[KMS.3] 실수로 삭제해서는 AWS KMS keys안 됩니다.

[KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.

[Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

[Macie.1] Amazon Macie가 활성화되어야 합니다.

[Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.

[MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.

[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.

[MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.

[MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다

[MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다

[MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다

[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.

[Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.

[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

[Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.

[Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.

[Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.

[NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.

[NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.

[NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.

[NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.

[NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.

[NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다

[Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

[Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.

[Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.

[Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.

[Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.

[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.

[PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.

[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

[RDS.1] RDS 스냅샷은 비공개여야 합니다.

[RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다.

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.

[RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.

[RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.

[RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.

[RDS.9] RDS DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.

[RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.

[RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.

[RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.

[RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.

[RDS.16] Aurora DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다.

[RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

[RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.

[RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.

[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.

[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.

[RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.

[RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다

[RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.

[RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다

[RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다

[RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다

[RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다

[RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다

[RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다

[RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다

[RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.

[RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

[Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

[Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.

[Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.

[Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다

[Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.

[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다

[Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.

[Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다

[RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다

[RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다

[RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다

[RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다

[RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다

[S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다

[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다

[S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.

[S3.6] S3 범용 버킷 정책은 다른에 대한 액세스를 제한해야 합니다. AWS 계정

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.9] S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다

[S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다

[S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다

[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다

[S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

[SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.

[SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.

[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

[SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다

[SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다

[SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

[SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

[SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

[SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

[SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

[SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.

[SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

[SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.

[SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.

[SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.

[SecretsManager.1] Secrets Manager 암호에는 자동 교체가 활성화되어 있어야 합니다.

[SecretsManager.2] 자동 교체로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.

[SecretsManager.3] 사용하지 않는 Secrets Manager 암호 삭제

[SecretsManager.4] Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다.

[ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.

[SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.

[SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.

[SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.

[SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다

[SSM.1] Amazon EC2 인스턴스는에서 관리해야 합니다.AWS Systems Manager

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.4] SSM 문서는 공개해서는 안 됩니다.

[SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다

[SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다

[StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.

[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.

[Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다

[WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

[WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.

[WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.

[WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.

[WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.

[WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

[WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.

[WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.

[WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## Security Hub CSPM의 AI 보안 모범 사례 표준

AI 보안 모범 사례 표준은 배포된 AI 리소스가 보안 모범 사례와 일치하지 않는 경우를 감지하는 자동화된 보안 검사 세트입니다. 보안 전문가가 개발한 AWS 이 표준은 AI 워크로드가 권장 보안 구성에서 벗어나는 영역을 식별하는 데 도움이 되는 엄선된 제어 세트를 제공합니다.

AWS Security Hub CSPM의 AI 보안 모범 사례 표준에는 리소스를 지속적으로 평가하는 제어가 포함되어 있습니다. 제어는 네트워크 격리, 저장 및 전송 중 암호화, VPC 배치, AWS KMS 키 사용 및 프라이빗 레지스트리 요구 사항을 포함하되 이에 국한되지 않는 보안 도메인을 다룹니다. 각 제어에는 제어가 적용되는 보안 기능을 반영하는 범주가 할당됩니다. 범주 목록 및 추가 세부 정보는 Security Hub CSPM의 제어 범주 섹션을 참조하세요.

AI 보안 모범 사례 표준의 Amazon 리소스 이름(ARN)은 입니다. `arn:aws:securityhub:region::standards/ai-security-best-practices/v/1.0.0`여기서 *region*은 해당의 리전 코드입니다 AWS 리전. 또한 Security Hub CSPM API의 GetEnabledStandards 작업을 사용하여 현재 활성화된 표준의 ARN을 검색할 수도 있습니다.

표준에 적용되는 제어

다음 목록은 AI AWS 보안 모범 사례 표준(v1.0.0)에 적용되는 Security Hub CSPM 제어를 지정합니다. 제어의 세부 정보를 검토하려면 해당 제어를 선택하세요.

- [Bedrock.1] Amazon Bedrock 데이터 소스는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [BedrockAgentCore.7] Bedrock AgentCore 사용자 지정 코드 인터프리터는 프라이빗 네트워크 구성을 사용해야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.20] SageMaker 모델 설명 가능성 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.21] SageMaker 노트북 인스턴스는 고객 관리형 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.22] SageMaker 모니터링 일정에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.23] SageMaker 추론 실험에는 고객 관리형 AWS KMS 키로 암호화된 인스턴스 스토리지 볼륨이 있어야 합니다.
- [SageMaker.24] SageMaker 추론 실험에는 고객 관리형 AWS KMS 키로 암호화된 데이터 스토리지가 있어야 합니다.
- [SageMaker.25] SageMaker 모델 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

## AWS Security Hub CSPM의 리소스 태그 지정 표준

AWS Security Hub CSPM에서 개발한 AWS 리소스 태그 지정 표준은 AWS 리소스에 태그가 누락되었는지 확인하는 데 도움이 됩니다. 태그는 AWS 리소스를 구성하기 위한 메타데이터 역할을 하는 키-값 페어입니다. 대부분의 AWS 리소스에는 리소스를 생성하는 동안 또는 리소스를 생성한 후에 태그를 추가할 수 있는 옵션이 있습니다. 리소스의 예로는 Amazon CloudFront 배포, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, AWS Secrets Manager의 시크릿 등이 있습니다. 태그를 사용하면 AWS 리소스를 관리, 식별, 구성, 검색 및 필터링할 수 있습니다.

각 태그는 두 부분으로 구성됩니다.

- 태그 키 - 예: `CostCenter`, `Environment` 또는 `Project`. 태그 키는 대소문자를 구별합니다.
- 태그 값 - 예: `111122223333` 또는 `Production`. 태그 키처럼 태그 값은 대/소문자를 구별합니다.

태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. AWS 리소스에 태그를 추가하는 방법에 대한 자세한 내용은 리소스 태그 지정 AWS 및 태그 편집기 사용 설명서를 참조하세요.

Security Hub CSPM의 AWS 리소스 태그 지정 표준에 적용되는 각 제어에 대해 지원되는 파라미터를 선택적으로 사용하여 제어에서 확인할 태그 키를 지정할 수 있습니다. 태그 키를 지정하지 않으면 제어는 하나 이상의 태그 키가 존재하는지만 확인하고 리소스에 태그 키가 없는 경우 제어가 실패합니다.

AWS 리소스 태그 지정 표준을 활성화하기 전에에서 리소스 기록을 활성화하고 구성하는 것이 중요합니다 AWS Config. 리소스 기록을 구성할 때는 표준에 적용되는 제어에서 확인하는 모든 유형의 AWS 리소스에 대해서도 리소스 기록을 활성화해야 합니다. 그렇지 않으면 Security Hub CSPM이 적절한 리소스를 평가하고 표준에 적용되는 제어에 대한 정확한 조사 결과를 생성하지 못할 수 있습니다. 기록할 리소스 유형의 목록을 포함하여 자세한 내용은 제어 조사 결과에 필요한 AWS Config리소스 섹션을 참조하세요.

AWS 리소스 태그 지정 표준을 활성화하면 표준에 적용되는 제어에 대한 조사 결과를 수신하기 시작합니다. Security Hub CSPM이 다른 활성화된 표준에 적용되는 제어와 동일한 AWS Config 서비스 연결 규칙을 사용하는 제어에 대한 조사 결과를 생성하는 데 최대 18시간이 걸릴 수 있습니다. 자세한 내용은 보안 검사 실행 예약 단원을 참조하십시오.

AWS 리소스 태그 지정 표준의 Amazon 리소스 이름(ARN)은 입니다. `arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0`여기서 *region*은 해당의 리전 코드입니다 AWS 리전. 또한 Security Hub CSPM API의 GetEnabledStandards 작업을 사용하여 현재 활성화된 표준의 ARN을 검색할 수도 있습니다.

> **Note**
>
> 아시아 태평양(뉴질랜드) 및 아시아 태평양(타이베이) 리전에서는 AWS 리소스 태그 지정 표준을 사용할 수 없습니다.

### 표준에 적용되는 제어

다음 목록은 AWS 리소스 태그 지정 표준(v1.0.0)에 적용되는 AWS Security Hub CSPM 제어를 지정합니다. 제어의 세부 정보를 검토하려면 해당 제어를 선택하세요.

- [ACM.3] ACM 인증서에 태그를 지정해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.

- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.4]AWS AppSyncGraphQL APIs 태그를 지정해야 합니다.
- [Athena.2] Athena 데이터 카탈로그에 태그를 지정해야 합니다.
- [Athena.3] Athena 작업 그룹에 태그를 지정해야 합니다.
- [AutoScaling.10] EC2 Auto Scaling 그룹에 태그를 지정해야 합니다.
- [Backup.2]AWS Backup복구 지점에 태그를 지정해야 합니다.
- [Backup.3] AWS Backup볼트에 태그를 지정해야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Backup.5]AWS Backup백업 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [CloudFormation.2] CloudFormation 스택에 태그를 지정해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudTrail.9] CloudTrail 추적에는 태그를 지정해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.

- [DynamoDB.5] DynamoDB 테이블에 태그를 지정해야 합니다.
- [EC2.33] EC2 Transit Gateway Attachment에 태그를 지정해야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.35] EC2 네트워크 인터페이스에 태그를 지정해야 합니다.
- [EC2.36] EC2 고객 게이트웨이에 태그를 지정해야 합니다.
- [EC2.37] EC2 탄력적 IP 주소에 태그를 지정해야 합니다.
- [EC2.38] EC2 인스턴스에 태그를 지정해야 합니다.
- [EC2.39] EC2 인터넷 게이트웨이에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.41] EC2 네트워크 ACL에 태그를 지정해야 합니다.
- [EC2.42] EC2 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.43] EC2 보안 그룹에 태그를 지정해야 합니다.
- [EC2.44] EC2 서브넷에 태그를 지정해야 합니다.
- [EC2.45] EC2 볼륨에 태그를 지정해야 합니다.
- [EC2.46] Amazon VPC에 태그를 지정해야 합니다.
- [EC2.47] Amazon VPC 엔드포인트 서비스에 태그를 지정해야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에 태그를 지정해야 합니다.
- [EC2.49] Amazon VPC 피어링 연결에 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에 태그를 지정해야 합니다.
- [EC2.52] EC2 전송 게이트웨이에 태그를 지정해야 합니다.
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECS.13] ECS 서비스에 태그를 지정해야 합니다
- [ECS.14] ECS 클러스터에 태그를 지정해야 합니다.

- [ECS.15] ECS 작업 정의에 태그를 지정해야 합니다.
- [EFS .5] EFS 액세스 포인트에 태그를 지정해야 합니다.
- [EKS.6] EKS 클러스터에 태그를 지정해야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.
- [ES.9] Elasticsearch 도메인에 태그를 지정해야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.1]AWS Glue작업에 태그를 지정해야 합니다.
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPSets에 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에 태그를 지정해야 합니다.
- [IAM.23] IAM Access Analyzer 분석기에 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.

- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.2] Kinesis 스트림에 태그를 지정해야 합니다.
- [Lambda.6] Lambda 함수에는 태그를 지정해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [NetworkFirewall.7] 네트워크 방화벽에 태그를 지정해야 합니다.
- [NetworkFirewall.8] 네트워크 방화벽 정책에 태그를 지정해야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.28] RDS DB 클러스터에 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에 태그를 지정해야 합니다.
- [RDS.30] RDS DB 인스턴스에 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.32] RDS DB 스냅샷에 태그를 지정해야 합니다.
- [RDS.33] RDS DB 서브넷 그룹에 태그를 지정해야 합니다.
- [Redshift.11] Redshift 클러스터에 태그를 지정해야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에 태그를 지정해야 합니다.
- [Redshift.14] Redshift 클러스터 서브넷 그룹에 태그를 지정해야 합니다.
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다

- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SecretsManager.5] Secrets Manager 보안 암호에 태그를 지정해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SNS.3] SNS 주제에 태그를 지정해야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.1]AWS Transfer Family워크플로에 태그를 지정해야 합니다.
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다

## Security Hub CSPM의 CIS AWS 파운데이션 벤치마크

Center for Internet Security(CIS) AWS Foundations Benchmark는 일련의 보안 구성 모범 사례 역할을 합니다 AWS. 업계에서 인정받은 이러한 모범 사례는 명확한 단계별 구현 및 평가 절차를 제공합니다. 운영 체제에서 클라우드 서비스 및 네트워크 장치에 이르기까지 이 Benchmark의 제어 기능은 조직에서 사용하는 특정 시스템을 보호하는 데 도움이 됩니다.

AWS Security Hub CSPM은 CIS AWS Foundations Benchmark 버전 5.0.0, 3.0.0, 1.4.0 및 1.2.0을 지원합니다. 이 페이지에는 각 버전이 지원하는 보안 제어가 나열되어 있습니다. 또한 버전 비교도 제공합니다.

CIS AWS 파운데이션 벤치마크 버전 5.0.0

Security Hub CSPM은 CIS AWS 파운데이션 벤치마크 버전 5.0.0(v5.0.0)을 지원합니다. Security Hub CSPM은 CIS 보안 소프트웨어 인증 요구 사항을 충족했으며 다음 CIS Benchmark에 대해 CIS 보안 소프트웨어 인증을 받았습니다.

- CIS AWS 파운데이션 벤치마크용 CIS 벤치마크, v5.0.0, 레벨 1

- CIS AWS 파운데이션 벤치마크용 CIS 벤치마크, v5.0.0, 레벨 2

CIS AWS 파운데이션 벤치마크 버전 5.0.0에 적용되는 제어

[Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정

[CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

[CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.

[Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

[EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

[EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS

[EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support

[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.

[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.

[IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.

[IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.

[KMS.4]AWS KMS키 교체를 활성화해야 합니다.

[RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다.

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.

[S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다

[S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.

[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.

### CIS AWS 파운데이션 벤치마크 버전 3.0.0

Security Hub CSPM은 CIS AWS 파운데이션 벤치마크 버전 3.0.0(v3.0.0)을 지원합니다. Security Hub CSPM은 CIS 보안 소프트웨어 인증 요구 사항을 충족했으며 다음 CIS Benchmark에 대해 CIS 보안 소프트웨어 인증을 받았습니다.

- CIS AWS 파운데이션 벤치마크용 CIS 벤치마크, v3.0.0, 레벨 1
- CIS AWS 파운데이션 벤치마크용 CIS 벤치마크, v3.0.0, 레벨 2

#### CIS AWS 파운데이션 벤치마크 버전 3.0.0에 적용되는 제어

[Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정

[CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

[CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.

[Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

[EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

[EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support

[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.

[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.

[IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.

[IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.

[KMS.4]AWS KMS키 교체를 활성화해야 합니다.

[RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다.

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다

[S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.

[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.

CIS AWS 파운데이션 벤치마크 버전 1.4.0

Security Hub CSPM은 CIS AWS 파운데이션 벤치마크 버전 1.4.0(v1.4.0)을 지원합니다.

CIS AWS 파운데이션 벤치마크 버전 1.4.0에 적용되는 제어

[CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다.

[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.

[CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.

[CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

[CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다

[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인

[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

[CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인

[CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support

[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.

[KMS.4]AWS KMS키 교체를 활성화해야 합니다.

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

[S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다

[S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

CIS AWS 파운데이션 벤치마크 버전 1.2.0

Security Hub CSPM은 CIS AWS 파운데이션 벤치마크 버전 1.2.0(v1.2.0)을 지원합니다. Security Hub CSPM은 CIS 보안 소프트웨어 인증 요구 사항을 충족했으며 다음 CIS Benchmark에 대해 CIS 보안 소프트웨어 인증을 받았습니다.

- CIS AWS 파운데이션 벤치마크용 CIS 벤치마크, v1.2.0, 레벨 1
- CIS AWS 파운데이션 벤치마크용 CIS 벤치마크, v1.2.0, 레벨 2

CIS AWS 파운데이션 벤치마크 버전 1.2.0에 적용되는 제어

[CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다.

[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.

[CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.

[CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

[CloudWatch.2] 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.3] MFA 없는 로그인에 대해 관리 콘솔에 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다

[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인

[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

[CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인

[CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

[Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.

[IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.

[IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.

[IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.

[IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support

[KMS.4]AWS KMS키 교체를 활성화해야 합니다.

CIS AWS 파운데이션 벤치마크 버전 비교

이 섹션에서는 인터넷 보안 센터(CIS) AWS 기반 벤치마크인 v5.0.0, v3.0.0, v1.4.0 및 v1.2.0의 특정 버전 간의 차이점을 요약합니다. AWS Security Hub CSPM은 이러한 CIS AWS 파운데이션 벤치마크 버전을 각각 지원합니다. 그러나 보안 모범 사례를 최신 상태로 유지하려면 v5.0.0을 사용하는 것이 좋습니다. 여러 버전의 CIS AWS 파운데이션 벤치마크 표준을 동시에 활성화할 수 있습니다. 표준을 활성화하는 방법에 대한 자세한 내용은 보안 표준 활성화 섹션을 참조하세요. v5.0.0으로 업그레이드하려면 이전 버전을 비활성화하기 전에 먼저 활성화하는 것이 좋습니다. 이렇게 하면 보안 검사의 격차를 방지할 수 있습니다. AWS Organizations 와 Security Hub CSPM 통합을 사용하고 여러 계정에서 v5.0.0을 일괄 활성화하려는 경우 중앙 구성을 사용하는 것이 좋습니다.

각 버전의 CIS 요구 사항에 대한 제어 매핑

CIS AWS 파운데이션 벤치마크의 각 버전에서 지원하는 제어를 이해합니다.

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정 | 1.2 | 1.2 | 1.2 | 1.18 |
| [CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다. | 3.1 | 3.1 | 3.1 | 2.1 |
| [CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다. | 3.5 | 3.5 | 3.7 | 2.7 |
| [CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다. | 3.2 | 3.2 | 3.2 | 2.2 |
| [CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 3.4 | 2.4 |
| [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 3.3 | 2.3 |
| [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다. | 3.4 | 3.4 | 3.6 | 2.6 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.3 | 3.3 |
| [CloudWatch.2] 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 3.1 |
| [CloudWatch.3] MFA 없는 로그인에 대해 관리 콘솔에 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 3.2 |
| [CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.4 | 3.4 |
| [CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다 | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.5 | 3.5 |
| [CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.6 | 3.6 |
| [CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.7 | 3.7 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.8 | 3.8 |
| [CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.9 | 3.9 |
| [CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.10 | 3.10 |
| [CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.11 | 3.11 |
| [CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.12 | 3.12 |
| [CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.13 | 3.13 |
| [CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 4.14 | 3.14 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. | 3.3 | 3.3 | 3.5 | 2.5 |
| [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다. | 5.5 | 5.4 | 5.3 | 4.3 |
| [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다. | 3.7 | 3.7 | 3.9 | 2.9 |
| [EC2.7] EBS 기본 암호화를 활성화해야 합니다. | 5.1.1 | 2.2.1 | 2.2.1 | 지원되지 않음 |
| [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다. | 5.7 | 5.6 | 지원되지 않음 | 지원되지 않음 |
| [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다. | 지원되지 않음 - 요구 사항 5.3 및 5.4로 대체됨 | 지원되지 않음 - 요구 사항 5.2 및 5.3으로 대체됨 | 지원되지 않음 - 요구 사항 5.2 및 5.3으로 대체됨 | 4.1 |
| [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다. | 지원되지 않음 - 요구 사항 5.3 및 5.4로 대체됨 | 지원되지 않음 - 요구 사항 5.2 및 5.3으로 대체됨 | 지원되지 않음 - 요구 사항 5.2 및 5.3으로 대체됨 | 4.2 |
| [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다. | 5.2 | 5.1 | 5.1 | 지원되지 않음 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다 | 5.3 | 5.2 | 지원되지 않음 | 지원되지 않음 |
| [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다 | 5.4 | 5.3 | 지원되지 않음 | 지원되지 않음 |
| [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS | 2.3.1 | 2.4.1 | 지원되지 않음 | 지원되지 않음 |
| [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다. | 2.3.1 | 지원되지 않음 | 지원되지 않음 | 지원되지 않음 |
| [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다. | 지원되지 않음 | 지원되지 않음 | 1.16 | 1.22 |
| [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다. | 1.14 | 1.15 | 지원되지 않음 | 1.16 |
| [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다. | 1.13 | 1.14 | 1.14 | 1.4 |
| [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다. | 1.3 | 1.4 | 1.4 | 1.12 |
| [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다. | 1.9 | 1.10 | 1.10 | 1.2 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다. | 1.5 | 1.6 | 1.6 | 1.14 |
| [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다. | 지원되지 않음 - 대신 [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다. 참조 | 지원되지 않음 - 대신 [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다. 참조 | 지원되지 않음 - 대신 [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다. 참조 | 1.3 |
| [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다. | 1.4 | 1.5 | 1.5 | 1.13 |
| [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 1.5 |
| [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 1.6 |
| [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 1.7 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 1.8 |
| [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다. | 1.7 | 1.8 | 1.8 | 1.9 |
| [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다. | 1.8 | 1.9 | 1.9 | 1.10 |
| [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 1.11 |
| [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support | 1.16 | 1.17 | 1.17 | 1.2 |
| [IAM.20] 루트 사용자의 사용을 피합니다. | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 지원되지 않음 - CIS가 이 요구 사항을 제거했음 | 1.1 |
| [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다. | 1.11 | 1.12 | 1.12 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다. | 1.18 | 1.19 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다. | 1.21 | 1.22 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다. | 1.19 | 1.20 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [KMS.4]AWS KMS키 교체를 활성화해야 합니다. | 3.6 | 3.6 | 3.8 | 2.8 |
| [Macie.1] Amazon Macie가 활성화되어야 합니다. | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 | 지원되지 않음 - 수동 확인 |
| [RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다. | 2.2.3 | 2.3.3 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다. | 2.2.1 | 2.3.1 | 2.3.1 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다. | 2.2.4 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다. | 2.2.2 | 2.3.2 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다. | 2.2.4 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다 | 2.1.4 | 2.1.4 | 2.1.5 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다. | 2.1.1 | 2.1.1 | 2.1.2 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |
| [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다. | 2.1.4 | 2.1.4 | 2.1.5 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |

| 제어 ID 및 제목 | CIS v5.0.0 요구 사항 | CIS v3.0.0 요구 사항 | CIS v1.4.0 요구 사항 | CIS v1.2.0 요구 사항 |
|---|---|---|---|---|
| [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다. | 2.1.2 | 2.1.2 | 2.1.3 | 지원되지 않음 - CIS가 이 요구 사항을 이후 버전에 추가했음 |

CIS AWS 파운데이션 벤치마크용 ARNs

하나 이상의 CIS AWS 파운데이션 벤치마크 버전을 활성화하면 AWS 보안 조사 결과 형식(ASFF)으로 조사 결과를 받기 시작합니다. ASFF에서 각 버전은 다음 Amazon 리소스 이름(ARN)을 사용합니다.

CIS AWS 파운데이션 벤치마크 v5.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/5.0.0
```

CIS AWS 파운데이션 벤치마크 v3.0.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/3.0.0
```

CIS AWS 파운데이션 벤치마크 v1.4.0

```
arn:aws:securityhub:region::standards/cis-aws-foundations-benchmark/v/1.4.0
```

CIS AWS 파운데이션 벤치마크 v1.2.0

```
arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Security Hub CSPM API의 GetEnabledStandards 작업을 사용하여 활성화된 표준의 ARN을 찾을 수 있습니다.

앞의 값은 `StandardsArn`에 대한 것입니다. 그러나 `StandardsSubscriptionArn`은 리전에서 BatchEnableStandards를 직접적으로 호출하여 표준을 구독할 때 Security Hub CSPM이 생성하는 표준 구독 리소스를 나타냅니다.

> **Note**
>
> CIS AWS 파운데이션 벤치마크 버전을 활성화하면 Security Hub CSPM이 다른 활성화된 표준에서 활성화된 제어와 동일한 AWS Config 서비스 연결 규칙을 사용하는 제어에 대한 결과를 생성하는 데 최대 18시간이 걸릴 수 있습니다. 제어 조사 결과 생성 일정에 대한 자세한 내용은 보안 검사 실행 예약 섹션을 참조하세요.

통합 제어 조사 결과를 켜면 조사 결과 필드가 달라집니다. 해당 차이점에 대한 자세한 내용은 ASFF 필드 및 값에 대한 통합의 영향 섹션을 참조하세요. 샘플 제어 조사 결과는 제어 조사 결과 샘플 섹션을 참조하세요.

Security Hub CSPM에서 지원되지 않는 CIS 요구 사항

위 표에 나와 있듯이 Security Hub CSPM은 모든 버전의 CIS AWS 파운데이션 벤치마크에서 모든 CIS 요구 사항을 지원하지 않습니다. 지원되지 않는 요구 사항은 대부분 수동으로 AWS 리소스 상태를 검토해야만 평가할 수 있습니다.

## Security Hub CSPM의 NIST SP 800-53 개정 5

NIST 특별 간행물 800-53 개정 5(NIST SP 800-53 개정 5)는 미국 상무부 산하 기관인 국립 표준 기술 연구소(NIST)에서 개발한 사이버 보안 및 규정 준수 프레임워크입니다. 이 규정 준수 프레임워크는 정보 시스템 및 중요 리소스의 기밀성, 무결성, 가용성을 보호하기 위한 보안 및 개인 정보 보호 요구 사항의 카탈로그를 제공합니다. 미국 연방 정부 기관 및 계약업체는 시스템 및 조직을 보호하기 위해 이러한 요구 사항을 준수해야 합니다. 또한 민간 조직도 사이버 보안 위험을 줄이기 위한 지침 프레임워크로 해당 요구 사항을 자발적으로 사용할 수 있습니다. 이 프레임워크 및 해당 요구 사항에 대한 자세한 내용은 NIST 컴퓨터 보안 리소스 센터에서 NIST SP 800-53 개정 5를 참조하세요.

AWS Security Hub CSPM은 NIST SP 800-53 개정 5 요구 사항의 하위 집합을 지원하는 보안 제어를 제공합니다. 제어는 특정 AWS 서비스 및 리소스에 대한 자동 보안 검사를 수행합니다. 이러한 제어를 활성화하고 관리하기 위해 Security Hub CSPM에서 NIST SP 800-53 개정 5 프레임워크를 표준으로 활성화할 수 있습니다. Security Hub CSPM 제어는 수동 검사가 필요한 NIST SP 800-53 개정 5 요구 사항을 지원하지 않습니다.

다른 프레임워크와 달리 NIST SP 800-53 개정 5 프레임워크는 요구 사항 평가 방법에 대한 규범이 아닙니다. 대신, 이 프레임워크는 지침을 제공합니다. Security Hub CSPM에서 NIST SP 800-53 개정 5 표준 및 제어는 이러한 지침에 대한 서비스의 이해를 나타냅니다.

주제

- 표준에 적용되는 제어에 대한 리소스 기록 구성
- 표준에 적용되는 제어 결정

표준에 적용되는 제어에 대한 리소스 기록 구성

조사 결과의 적용 범위와 정확도를 최적화하려면 AWS Security Hub CSPM에서 NIST SP 800-53 개정 5 표준을 활성화하기 AWS Config 전에에서 리소스 기록을 활성화하고 구성하는 것이 중요합니다. 리소스 기록을 구성할 때는 표준에 적용되는 제어에서 확인하는 모든 유형의 AWS 리소스에 대해서도 리소스 기록을 활성화해야 합니다. 이는 주로 변경 트리거 일정 유형을 사용하는 제어에 필요합니다. 그러나 일정 유형이 주기적인 일부 제어에도 리소스 기록이 필요합니다. 리소스 기록이 활성화되지 않았거나 제대로 구성되지 않은 경우 Security Hub CSPM은 적절한 리소스를 평가하고 표준에 적용되는 제어에 대한 정확한 결과를 생성하지 못할 수 있습니다.

Security Hub CSPM이에서 리소스 기록을 사용하는 방법에 대한 자세한 내용은 섹션을 AWS Config참조하세요Security Hub CSPM AWS Config 에 대한 활성화 및 구성. 에서 리소스 레코딩을 구성하는 방법에 대한 자세한 내용은 AWS Config 개발자 안내서의 구성 레코더 작업을 AWS Config참조하세요.

다음 표에서는 Security Hub CSPM의 NIST SP 800-53 개정 5 표준에 적용되는 제어에 대해 기록할 리소스 유형을 보여줍니다.

| AWS 서비스 | 조건 키 |
| --- | --- |
| Amazon API Gateway | `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage` |
| AWS AppSync | `AWS::AppSync::GraphQLApi` |
| AWS Backup | `AWS::Backup::RecoveryPoint` |
| Amazon Bedrock 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 서비스 | 조건 키 |
| --- | --- |
| 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 오토 스케일링 | `AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration` |
| Amazon Elastic Container Registry(Amazon ECR) | `AWS::ECR::Repository` |
| 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` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |
| Amazon MQ | `AWS::AmazonMQ::Broker` |
| AWS Network Firewall | `AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup` |
| Amazon OpenSearch Service | `AWS::OpenSearch::Domain` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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(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` |
| AWS Secrets Manager | `AWS::SecretsManager::Secret` |
| AWS Transfer Family | `AWS::Transfer::Connector` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |

표준에 적용되는 제어 결정

다음 목록은 NIST SP 800-53 개정 5 요구 사항을 지원하고 AWS Security Hub CSPM의 NIST SP 800-53 개정 5 표준에 적용되는 제어를 지정합니다. 제어가 지원하는 특정 요구 사항에 대한 세부 정보를 보려면 해당 제어를 선택합니다. 그런 다음 제어 세부 정보에서 관련 요구 사항 필드를 참조하세요. 이 필드는 제어가 지원하는 각 NIST 요구 사항을 표시합니다. 필드에 특정 NIST 요구 사항이 지정되지 않은 경우 제어가 요구 사항을 지원하지 않는 것입니다.

- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [APIGateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [PCI.AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.

- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다.
- [CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.
- [CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.
- [CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CloudWatch.15] CloudWatch 경보에는 지정된 구성되어 있어야 합니다.
- [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.

- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.
- [DynamoDB.2] DynamoDB 테이블에는 시점 복구가 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원 가능하도록 구성해서는 안 됩니다.
- [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.
- [EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

- [EC2.7] EBS 기본 암호화를 활성화해야 합니다.
- [EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.
- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.
- [EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.
- [EC2.20] a AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.

- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.4] Application Load Balancer는 잘못된 http 헤더를 삭제하도록 구성되어야 합니다.
- [ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.
- [ELB.6] 애플리케이션, 게이트웨이, Network Load Balancers에는 삭제 보호가 활성화되어 있어야 합니다.
- [ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.
- [ELB.8] SSL AWS Config리스너가 있는 Classic Load Balancer는 강력한 요구 사항이 있는 사전 정의된 보안 정책을 사용해야 합니다.
- [ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] Application Load Balancer는 AWS WAF 웹 ACL과 연결되어야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.
- [ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.

- [ES.8] Elasticsearch 도메인에 대한 연결은 TLS 보안 정책을 사용하여 암호화해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.1] GuardDuty를 활성화해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.3] 실수로 삭제해서는 AWS KMS keys안 됩니다.
- [KMS.4]AWS KMS키 교체를 활성화해야 합니다.
- [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
- [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.
- [Lambda.3] Lambda 함수는 VPC에 있어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.

- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.

- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다.
- [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.
- [RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.
- [RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.
- [RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.9] RDS DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.
- [RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] Aurora DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

- [RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다
- [S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.
- [S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다
- [S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.
- [S3.6] S3 범용 버킷 정책은 다른에 대한 액세스를 제한해야 합니다. AWS 계정
- [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다
- [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.
- [S3.9] S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다

- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.14] S3 범용 버킷에는 버전 관리가 활성화되어 있어야 합니다
- [S3.15] S3 범용 버킷에는 Object Lock이 활성화되어 있어야 합니다.
- [S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys
- [S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SecretsManager.1] Secrets Manager 암호에는 자동 교체가 활성화되어 있어야 합니다.
- [SecretsManager.2] 자동 교체로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 암호 삭제
- [SecretsManager.4] Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SNS.1] SNS 주제는를 사용하여 유휴 시 암호화되어야 합니다.AWS KMS
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SSM.1] Amazon EC2 인스턴스는에서 관리해야 합니다.AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11]AWS WAF웹 ACL 로깅을 활성화해야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.

## Security Hub CSPM의 NIST SP 800-171 개정 2

NIST 특별 간행물 800-171 개정 2(NIST SP 800-171 개정 2)는 미국 상무부 산하 기관인 국립 표준 기술 연구소(NIST)에서 개발한 사이버 보안 및 규정 준수 프레임워크입니다. 이 규정 준수 프레임워크는 미국 연방 정부에 속하지 않는 시스템 및 조직에서 통제된 미분류 정보의 기밀성을 보호하기 위한 권장 보안 요구 사항을 제공합니다. 통제된 미분류 정보(CUI라고도 함)는 연방 정부의 분류 기준을 충족하지 않지만 보호해야 하는 민감한 정보입니다. 민감한 정보로 간주되며 미국 연방 정부 또는 미국 연방 정부를 대신하여 기타 기관이 생성 또는 소유하는 정보입니다.

NIST SP 800-171 개정 2는 다음과 같은 경우 CUI의 기밀성을 보호하기 위한 권장 보안 요구 사항을 제공합니다.

- 정보가 비연방 시스템 및 조직에 상주하는 경우
- 비연방 조직이 연방 기관을 대신하여 정보를 수집 또는 유지하지 않거나 연방 기관을 대신하여 시스템을 사용 또는 운영하지 않는 경우
- CUI 레지스트리에 나열된 CUI 범주에 대한 권한 부여 법률, 규정 또는 정부 차원 정책에 규정된 CUI의 기밀성을 보호하기 위한 구체적인 보호 요구 사항이 없는 경우

요구 사항은 CUI를 처리, 저장 또는 전송하거나 구성 요소에 대한 보안 보호를 제공하는 비연방 시스템 및 조직의 모든 구성 요소에 적용됩니다. 자세한 내용은 NIST 컴퓨터 보안 리소스 센터에서 NIST SP 800-171 개정 2를 참조하세요.

AWS Security Hub CSPM은 NIST SP 800-171 개정 2 요구 사항의 하위 집합을 지원하는 보안 제어를 제공합니다. 제어는 특정 AWS 서비스 및 리소스에 대한 자동 보안 검사를 수행합니다. 이러한 제어를 활성화하고 관리하기 위해 Security Hub CSPM에서 NIST SP 800-171 개정 2 프레임워크를 표준으로

활성화할 수 있습니다. Security Hub CSPM 제어는 수동 검사가 필요한 NIST SP 800-171 개정 2 요구 사항을 지원하지 않습니다.

주제

- 표준에 적용되는 제어에 대한 리소스 기록 구성
- 표준에 적용되는 제어 결정

## 표준에 적용되는 제어에 대한 리소스 기록 구성

조사 결과의 적용 범위와 정확도를 최적화하려면 AWS Security Hub CSPM에서 NIST SP 800-171 개정 2 표준을 활성화하기 AWS Config 전에에서 리소스 기록을 활성화하고 구성하는 것이 중요합니다. 리소스 기록을 구성할 때는 표준에 적용되는 제어에서 확인하는 모든 유형의 AWS 리소스에 대해서도 리소스 기록을 활성화해야 합니다. 그렇지 않으면 Security Hub CSPM이 적절한 리소스를 평가하고 표준에 적용되는 제어에 대한 정확한 조사 결과를 생성하지 못할 수 있습니다.

Security Hub CSPM이에서 리소스 기록을 사용하는 방법에 대한 자세한 내용은 섹션을 AWS Config참조하세요Security Hub CSPM AWS Config 에 대한 활성화 및 구성. 에서 리소스 레코딩을 구성하는 방법에 대한 자세한 내용은 AWS Config 개발자 안내서의 구성 레코더 작업을 AWS Config참조하세요.

다음 표에서는 Security Hub CSPM의 NIST SP 800-171 개정 2 표준에 적용되는 제어에 대해 기록할 리소스 유형을 보여줍니다.

| AWS 서비스 | 조건 키 |
| --- | --- |
| AWS Certificate Manager(ACM) | `AWS::ACM::Certificate` |
| Amazon API Gateway | `AWS::ApiGateway::Stage` |
| Amazon CloudFront | `AWS::CloudFront::Distribution` |
| Amazon CloudWatch | `AWS::CloudWatch::Alarm` |
| Amazon Elastic Compute Cloud(Amazon EC2) | `AWS::EC2::ClientVpnEndpoint` , `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` , `AWS::EC2::VPC` , `AWS::EC2::VPNConnection` |
| Elastic Load Balancing | `AWS::ElasticLoadBalancing::LoadBalancer` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |
| Amazon Simple Storage Service(Amazon S3) | `AWS::S3::Bucket` |
| Amazon Simple Notification Service(Amazon SNS) | `AWS::SNS::Topic` |
| AWS Systems Manager(SSM) | `AWS::SSM::PatchCompliance` |
| AWS WAF | `AWS::WAFv2::RuleGroup` |

표준에 적용되는 제어 결정

다음 목록은 NIST SP 800-171 개정 2 요구 사항을 지원하고 AWS Security Hub CSPM의 NIST SP 800-171 개정 2 표준에 적용되는 제어를 지정합니다. 제어가 지원하는 특정 요구 사항에 대한 세부 정보를 보려면 해당 제어를 선택합니다. 그런 다음 제어 세부 정보에서 관련 요구 사항 필드를 참조하세요. 이 필드는 제어가 지원하는 각 NIST 요구 사항을 표시합니다. 필드에 특정 NIST 요구 사항이 지정되지 않은 경우 제어가 요구 사항을 지원하지 않는 것입니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.
- [CloudTrail.3] 하나 이상의 CloudTrail 추적을 활성화해야 합니다.
- [CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.
- [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

- [CloudWatch.2] 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다
- [CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인
- [CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다.
- [CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인
- [CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.15] CloudWatch 경보에는 지정된 구성되어 있어야 합니다.
- [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.
- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.
- [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.
- [EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.
- [EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.
- [EC2.20] a AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.8] SSL AWS Config리스너가 있는 Classic Load Balancer는 강력한 요구 사항이 있는 사전 정의된 보안 정책을 사용해야 합니다.
- [GuardDuty.1] GuardDuty를 활성화해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.
- [S3.6] S3 범용 버킷 정책은 다른에 대한 액세스를 제한해야 합니다. AWS 계정
- [S3.9] S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다

- [S3.14] S3 범용 버킷에는 버전 관리가 활성화되어 있어야 합니다
- [S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys
- [SNS.1] SNS 주제는를 사용하여 유휴 시 암호화되어야 합니다.AWS KMS
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.

## Security Hub CSPM의 PCI DSS

지불 카드 산업 데이터 보안 표준(PCI DSS)은 신용카드 및 직불카드 정보를 안전하게 처리하기 위한 일련의 규칙 및 지침을 제공하는 서드 파티 규정 준수 프레임워크입니다. PCI 보안 표준 위원회(SSC)에서 이 프레임워크를 작성하고 업데이트합니다.

AWS Security Hub CSPM은이 타사 프레임워크를 준수하는 데 도움이 되는 PCI DSS 표준을 제공합니다. 이 표준을 사용하여 카드 소지자 데이터를 처리하는 AWS 리소스의 보안 취약성을 발견할 수 있습니다. 카드 소지자 데이터 또는 민감한 인증 데이터를 저장, 처리 또는 전송하는 리소스가 있는 AWS 계정 은 이 표준을 활성화하는 것이 좋습니다. 이 표준은 PCI SSC의 평가를 통해 검증되었습니다.

Security Hub CSPM은 PCI DSS v3.2.1과 PCI DSS v4.0.1을 모두 지원합니다. 보안 모범 사례를 최신 상태로 유지하려면 v4.0.1을 사용하는 것이 좋습니다. 두 버전의 표준을 동시에 활성화할 수 있습니다. 표준을 활성화하는 방법에 대한 자세한 내용은 보안 표준 활성화 섹션을 참조하세요. 현재 v3.2.1을 사용하고 있지만 v4.0.1만 사용하려는 경우 이전 버전을 비활성화하기 전에 최신 버전을 활성화하세요. 이렇게 하면 보안 검사의 격차를 방지할 수 있습니다. AWS Organizations 와 Security Hub CSPM 통합을 사용하고 여러 계정에서 v4.0.1을 일괄 활성화하려는 경우 중앙 구성을 사용하여 활성화하는 것이 좋습니다.

다음 섹션에서는 PCI DSS v3.2.1 및 PCI DSS v4.0.1에 적용되는 제어를 자세히 소개합니다.

### PCI DSS v3.2.1에 적용되는 제어

다음 목록에서는 PCI DSS v3.2.1에 적용되는 Security Hub CSPM 제어를 보여줍니다. 제어의 세부 정보를 검토하려면 해당 제어를 선택하세요.

[PCI.AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

[CloudTrail.3] 하나 이상의 CloudTrail 추적을 활성화해야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

[CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다.

[CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.

[Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원 가능하도록 구성해서는 안 됩니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

[EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[GuardDuty.1] GuardDuty를 활성화해야 합니다.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.

[IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[KMS.4]AWS KMS키 교체를 활성화해야 합니다.

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

[Lambda.3] Lambda 함수는 VPC에 있어야 합니다.

[Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[RDS.1] RDS 스냅샷은 비공개여야 합니다.

[RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다.

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

[S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다

[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다

[S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.

[S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

[SSM.1] Amazon EC2 인스턴스는에서 관리해야 합니다.AWS Systems Manager

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT 여야 합니다.

PCI DSS v4.0.1에 적용되는 제어

다음 목록에서는 PCI DSS v4.0.1에 적용되는 Security Hub CSPM 제어를 보여줍니다. 제어의 세부 정보를 검토하려면 해당 제어를 선택하세요.

[ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.

[ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.

[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.

[AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.

[AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.

[Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.

[CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.

[CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

[CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

[CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.

[CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

[CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.

[CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

[CloudTrail.3] 하나 이상의 CloudTrail 추적을 활성화해야 합니다.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.

[CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.

[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

[DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

[DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.

[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.

[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.

[DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.

[DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

[EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.

[EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

[EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

[ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.

[ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.

[ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

[ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.

[ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.

[EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.

[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.

[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.

[EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.

[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다

[ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.

[ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.

[ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.

[ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.

[ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.

[ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.

[ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.

[ELB.4] Application Load Balancer는 잘못된 http 헤더를 삭제하도록 구성되어야 합니다.

[ELB.8] SSL AWS Config리스너가 있는 Classic Load Balancer는 강력한 요구 사항이 있는 사전 정의된 보안 정책을 사용해야 합니다.

[EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

[ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

[ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[ES.8] Elasticsearch 도메인에 대한 연결은 TLS 보안 정책을 사용하여 암호화해야 합니다.

[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.

[GuardDuty.1] GuardDuty를 활성화해야 합니다.

[GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.

[GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.

[GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.

[GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

[IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

[IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.

[IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.

[IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

[IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.

[IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support

[IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

[Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.

[Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.

[Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.

[Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.

[KMS.4]AWS KMS키 교체를 활성화해야 합니다.

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.

[MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.

[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.

[MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.

[Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.

[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.

[Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

[RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다.

[RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

[RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.

[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

[RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.

[RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.

[RDS.9] RDS DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

[Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.

[Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

[Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

[S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다

[S3.15] S3 범용 버킷에는 Object Lock이 활성화되어 있어야 합니다.

[S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys

[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.

[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.

[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.

[S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다

[S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

[S3.9] S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

[SecretsManager.1] Secrets Manager 암호에는 자동 교체가 활성화되어 있어야 합니다.

[SecretsManager.2] 자동 교체로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.

[SecretsManager.4] Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다.

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

[StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.

[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.

[WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

[WAF.11]AWS WAF웹 ACL 로깅을 활성화해야 합니다.

## Security Hub CSPM의 서비스 관리형 표준

서비스 관리형 표준은 다른에서 AWS 서비스 관리하지만 Security Hub CSPM에서 볼 수 있는 보안 표준입니다. 예를 들어 서비스 관리형 표준: AWS Control Tower는가 AWS Control Tower 관리하는 서비스 관리형 표준입니다. 서비스 관리형 표준은 다음과 같은 측면에서 AWS Security Hub CSPM이 관리하는 보안 표준과 다릅니다.

- 표준 생성 및 삭제 - 관리 서비스의 콘솔이나 API 또는 AWS CLI을(를) 사용하여 서비스 관리형 표준을 생성하고 삭제합니다. 이러한 방법 중 하나로 관리 서비스에서 표준을 작성하기 전까지는 표준이 Security Hub CSPM 콘솔에 나타나지 않으며 Security Hub CSPM API 또는 AWS CLI를 통해 액세스할 수 없습니다.
- 제어 자동 활성화 없음 - 서비스 관리형 표준을 만들 때 Security Hub CSPM 및 관리 서비스는 표준에 적용되는 제어를 자동으로 활성화하지 않습니다. 또한 Security Hub CSPM에서 표준에 대한 새로운 제어를 릴리스하더라도 자동으로 활성화되지는 않습니다. 이는 Security Hub CSPM이 관리하는

표준과는 다릅니다. Security Hub CSPM에서 제어를 구성하는 일반적인 방법에 대한 자세한 내용은 Security Hub CSPM의 보안 제어 이해 섹션을 참조하세요.

- 제어 활성화 및 비활성화 - 드리프트를 방지하려면 관리 서비스에서 제어를 활성화 및 비활성화하는 것이 좋습니다.
- 제어 가용성 – 관리 서비스는 서비스 관리형 표준의 일부로 사용할 수 있는 제어를 선택합니다. 사용 가능한 제어에는 기존 Security Hub CSPM 제어의 전부 또는 일부가 포함될 수 있습니다.

관리 서비스가 서비스 관리형 표준을 만들고 이에 대한 제어를 사용할 수 있게 만든 후에는 Security Hub CSPM 콘솔, Security Hub CSPM API 또는 AWS CLI에서 제어 조사 결과, 제어 상태 및 표준 보안 점수에 액세스할 수 있습니다. 이 정보의 일부 또는 전부는 관리 서비스에서도 확인할 수 있습니다.

다음 목록에서 서비스 관리형 표준을 선택하면 해당 표준에 대한 자세한 내용을 볼 수 있습니다.

서비스 관리형 표준

- 서비스 관리형 표준: AWS Control Tower

서비스 관리형 표준: AWS Control Tower

이 섹션에서는 서비스 관리형 표준에 대한 정보를 제공합니다 AWS Control Tower.

서비스 관리형 표준이란 무엇입니까 AWS Control Tower?

서비스 관리형 표준: Security Hub 제어의 하위 집합을 지원하는를 AWS Control Tower 관리하는 서비스 관리형 표준 AWS Control Tower 입니다. 이 표준은 AWS Security Hub CSPM 및 사용자를 위해 설계되었습니다 AWS Control Tower. 이를 통해 AWS Control Tower 서비스에서 Security Hub CSPM의 탐지 제어를 구성할 수 있습니다.

탐지 제어 기능은 AWS 계정내의 리소스 비준수(예제: 잘못된 구성)를 감지합니다.

> **Tip**
>
> 서비스 관리형 표준은 AWS Security Hub CSPM이 관리하는 표준과 다릅니다. 예를 들어, 관리 서비스에서 서비스 관리형 표준을 만들고 삭제해야 합니다. 자세한 내용은 Security Hub CSPM의 서비스 관리형 표준 단원을 참조하십시오.

를 통해 Security Hub CSPM 제어를 활성화하면 AWS Control Tower Control Tower는 아직 활성화되지 않은 경우 해당 특정 계정 및 리전에서 Security Hub CSPM도 활성화합니다. Security Hub CSPM

콘솔 및 API에서 표준이 활성화된 후 다른 Security Hub CSPM 표준과 AWS Control Tower 함께 서비스 관리형 표준을 볼 수 있습니다 AWS Control Tower.

이 표준에 대한 자세한 내용은 AWS Control Tower 사용 설명서의 Security Hub CSPM 제어를 참조하세요.

표준 생성

이 표준은 Security Hub CSPM 제어를 활성화한 경우에만 Security Hub CSPM에서 사용할 수 있습니다 AWS Control Tower. AWS Control Tower 는 다음 방법 중 하나를 사용하여 적용 가능한 제어를 처음 활성화할 때 표준을 생성합니다.

- AWS Control Tower 콘솔
- AWS Control Tower API(`EnableControl`API 호출)
- AWS CLI (`enable-control`명령 실행)

를 통해 Security Hub CSPM 제어를 활성화할 때 Security Hub CSPM을 아직 활성화하지 않은 AWS Control Tower경우는 해당 특정 계정 및 리전에서 Security Hub CSPM AWS Control Tower 도 활성화합니다.

Control Catalog에서 제어 ID로 Security Hub CSPM 제어를 식별하려면의 필드를 사용할 수 `Implementation.Identifier` 있습니다 AWS Control Tower. 이 필드는 Security Hub CSPM 제어 ID에 매핑되며 특정 제어 ID를 필터링하는 데 사용할 수 있습니다. 에서 특정 Security Hub CSPM 제어(예: "CodeBuild.1")에 대한 제어 메타데이터를 검색하려면 `ListControls` API를 사용할 AWS Control Tower수 있습니다.

```
aws controlcatalog list-controls --filter '{"Implementations":
{"Identifiers":["CodeBuild.1"],"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Security Hub CSPM 콘솔, Security Hub CSPM API 또는 먼저 위의 방법 중 하나를 AWS Control Tower 사용하여 Security Hub CSPM 제어를 설정하고 AWS Control Tower 활성화하지 AWS CLI 않으면이 표준을 보거나 액세스할 수 없습니다.

이 표준은를 사용할 수 AWS 리전 있는 에서만 사용할 수 AWS Control Tower 있습니다.

표준의 제어 활성화 및 비활성화

를 통해 Security Hub CSPM 제어를 활성화 AWS Control Tower 하고 서비스 관리형 표준: AWS Control Tower 표준이 생성된 후 Security Hub CSPM에서 표준 및 사용 가능한 제어를 볼 수 있습니다.

Security Hub CSPM이 서비스 관리형 표준: AWS Control Tower 표준에 새 제어를 추가하면 표준이 활성화된 고객에게 자동으로 활성화되지 않습니다. 다음 방법 중 하나를 AWS Control Tower 사용하여에서 표준에 대한 제어를 활성화 및 비활성화해야 합니다.

- AWS Control Tower 콘솔
- AWS Control Tower API( `EnableControl` 및 `DisableControl` APIs 호출)
- AWS CLI ( `enable-control` 및 `disable-control` 명령 실행)

에서 제어의 활성화 상태를 변경하면 변경 AWS Control Tower사항이 Security Hub CSPM에도 반영됩니다.

그러나 Security Hub CSPM에서 제어를 비활성화하면 제어 드리프트가 AWS Control Tower 발생합니다. 의 제어 상태는 로 AWS Control Tower 표시됩니다`Drifted`. ResetEnabledControl API를 사용하여 드리프트에 있는 컨트롤을 재설정하거나 AWS Control Tower 콘솔에서 OU 재등록을 선택하거나 위의 방법 중 하나를 AWS Control Tower 사용하여에서 컨트롤을 비활성화하고 다시 활성화하여이 드리프트를 해결할 수 있습니다.

에서 활성화 및 비활성화 작업을 완료하면 제어 드리프트를 방지하는 AWS Control Tower 데 도움이 됩니다.

에서 제어를 활성화하거나 비활성화하면 AWS Control Tower작업이 관리되는 계정 및 리전에 적용됩니다 AWS Control Tower. Security Hub CSPM에서 제어를 활성화 및 비활성화하는 경우(이 표준에서는 권장되지 않음) 작업은 현재 계정 및 리전에만 적용됩니다.

> **Note**
>
> 중앙 구성은 서비스 관리형 표준을 관리하는 데 사용할 수 없습니다 AWS Control Tower. 이 표준에서는 AWS Control Tower 서비스만 사용하여 제어를 활성화 및 비활성화할 수 있습니다.

활성화 상태 및 제어 상태 보기

다음 방법 중 하나를 사용하여 제어의 활성화 상태를 볼 수 있습니다.

- Security Hub CSPM 콘솔, Security Hub CSPM API 또는 AWS CLI
- AWS Control Tower 콘솔
- AWS Control Tower 활성화된 제어 목록을 볼 수 있는 API(`ListEnabledControls`API 호출)
- AWS CLI 활성화된 제어 목록을 보려면(`list-enabled-controls`명령 실행)

Security Hub CSPM에서 해당 제어를 명시적으로 활성화하지 않는 한 `Disabled`에서 비활성화하는 제어 AWS Control Tower 는 Security Hub CSPM에서 활성화 상태가 입니다.

Security Hub CSPM은 제어 조사 결과의 워크플로 상태 및 규정 준수 상태를 기반으로 제어 상태를 계산합니다. 활성화 상태 및 제어 상태에 대한 자세한 내용은 Security Hub CSPM에서 제어 세부 정보 검토 섹션을 참조하세요.

Security Hub CSPM은 제어 상태를 기반으로 서비스 관리형 표준의 보안 점수를 계산합니다 AWS Control Tower. 이 점수는 Security Hub CSPM에서만 사용할 수 있습니다. 또한 Security Hub CSPM에서는 제어 조사 결과만 볼 수 있습니다. 표준 보안 점수 및 제어 조사 결과는에서 사용할 수 없습니다 AWS Control Tower.

> **Note**
>
> 서비스 관리형 표준:에 대한 제어를 활성화하면 AWS Control Tower Security Hub CSPM이 기존 AWS Config 서비스 연결 규칙을 사용하는 제어에 대한 조사 결과를 생성하는 데 최대 18시간이 걸릴 수 있습니다. Security Hub CSPM에서 다른 표준 및 제어를 활성화한 경우, 기존 서비스 연결 규칙이 있을 수 있습니다. 자세한 내용은 보안 검사 실행 예약 단원을 참조하십시오.

표준 삭제

다음 방법 중 하나를 사용하여 적용 가능한 모든 제어를 비활성화 AWS Control Tower 하여에서이 서비스 관리형 표준을 삭제할 수 있습니다.

- AWS Control Tower 콘솔
- AWS Control Tower API(`DisableControl`API 호출)
- AWS CLI (`disable-control`명령 실행)

모든 제어를 비활성화하면 AWS Control Tower의 모든 관리 계정 및 관리되는 리전의 표준이 삭제됩니다. 에서 표준을 삭제하면 Security Hub CSPM 콘솔의 표준 페이지에서 AWS Control Tower 제거되며 Security Hub CSPM API 또는를 사용하여 더 이상 액세스할 수 없습니다 AWS CLI.

> **Note**
>
> Security Hub CSPM의 표준에서 모든 제어를 비활성화해도 표준이 비활성화되거나 삭제되지는 않습니다.

Security Hub CSPM 서비스를 비활성화하면 서비스 관리형 표준 AWS Control Tower 및 활성화한 기타 표준이 제거됩니다.

서비스 관리형 표준의 결과 필드 형식: AWS Control Tower

서비스 관리형 표준을 생성하고 이에 대한 제어를 AWS Control Tower 활성화하면 Security Hub CSPM에서 제어 조사 결과를 수신하기 시작합니다. Security Hub CSPM은 제어 조사 결과를 AWS 보안 조사 결과 형식(ASFF)으로 보고합니다. 다음은 이 표준의 Amazon 리소스 이름(ARN) 및 `GeneratorId`에 대한 ASFF 값입니다.

- 표준 ARN – `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`

서비스 관리형 표준:에 대한 샘플 결과는 섹션을 AWS Control Tower참조하세요제어 조사 결과 샘플.

서비스 관리형 표준에 적용되는 제어: AWS Control Tower

서비스 관리형 표준: AWS 기본 보안 모범 사례(FSBP) 표준의 일부인 제어의 하위 집합을 AWS Control Tower 지원합니다. 실패 조사 결과에 대한 문제 해결 단계를 포함하여 이에 대한 정보를 보려면 제어를 선택하세요.

어떤 Security Hub CSPM 제어가 지원되는 AWS Control Tower지 확인하려면 다음 방법 중 하나를 사용할 수 있습니다.

- AWS 필터링할 수 있는 Control Catalog 콘솔 “`Control owner = AWS Security Hub`”
- AWS 에서 `Implementations` 확인할 필터가 있는 Control Catalog API(`ListControls`API 호출)는 `Types`입니다. `AWS::SecurityHub::SecurityControl`
- AWS CLI 용 필터를 사용하여 (`list-controls`명령 실행) `Implementations` CLI 명령 예제:

```
aws controlcatalog list-controls --filter '{"Implementations":{"Types":
["AWS::SecurityHub::SecurityControl"]}}'
```

Control Tower 표준을 통해 활성화된 경우 Security Hub CSPM 제어에 대한 리전별 제한은 기본 제어에 대한 리전별 제한과 일치하지 않을 수 있습니다.

Security Hub CSPM에서 계정에서 통합 제어 조사 결과가 꺼져 있는 경우 생성된 조사 결과의 `ProductFields.ControlId` 필드는 표준 기반 제어 ID를 사용합니다. 표준 기반 제어 ID는 CT.***ControlId***(예제: CT.CodeBuild.1)로 형식이 지정됩니다.

이 표준에 대한 자세한 내용은 AWS Control Tower 사용 설명서의 Security Hub CSPM 제어를 참조하세요.

## 보안 표준 활성화

AWS Security Hub CSPM에서 보안 표준을 활성화하면 Security Hub CSPM은 표준에 적용되는 모든 제어를 자동으로 생성하고 활성화합니다. Security Hub CSPM은 또한 제어에 대한 보안 검사를 실행하고 조사 결과를 생성하기 시작합니다.

조사 결과의 적용 범위와 정확도를 최적화하려면 표준을 활성화 AWS Config 하기 전에에서 리소스 기록을 활성화하고 구성합니다. 리소스 기록을 구성할 때는 표준에 적용되는 제어에서 확인하는 모든 유형의 리소스에도 리소스 기록을 활성화해야 합니다. 그렇지 않으면 Security Hub CSPM이 적절한 리소스를 평가하고 표준에 적용되는 제어에 대한 정확한 조사 결과를 생성하지 못할 수 있습니다. 자세한 내용은 Security Hub CSPM AWS Config 에 대한 활성화 및 구성 단원을 참조하십시오.

CIS Azure Foundations Benchmark v4.0.0과 같은 멀티클라우드 보안 표준은 AWS 표준과 요구 사항이 다릅니다. 멀티클라우드 표준에는 외부 클라우드 공급자를 위한 Security Hub CSPM 커넥터가 필요하며 구성 레코더를 구성 AWS Config 하거나 수동으로 생성할 필요가 없습니다. Security Hub CSPM 멀티클라우드 커넥터는 외부 클라우드 환경의 리소스를 평가하기 위해 서비스 연결 레코더를 자동으로 설정합니다.

표준을 활성화한 후 해당 표준에 적용되는 개별 제어를 비활성화하고 나중에 다시 활성화할 수 있습니다. 표준에서 제어를 사용하지 않도록 설정하면 Security Hub CSPM은 해당 제어에 대한 조사 결과 생성을 중지합니다. 또한 Security Hub CSPM은 표준에 대한 보안 점수를 계산할 때 해당 제어를 무시합니다. 보안 점수는 표준에 적용되고, 활성화되고, 평가 데이터가 있는 제어의 전체 수에 대한 평가를 통과한 제어의 백분율입니다.

표준을 활성화하면 Security Hub CSPM은 사용자가 Security Hub CSPM 콘솔의 요약 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 표준에 대한 예비 보안 점수를 계산합니다. 보안 점수는 콘솔에서 해당 페이지를 방문했을 때 활성화된 표준에 대해서만 생성됩니다. 또한 AWS Config 점수가 표시되려면에서 리소스 기록을 구성해야 합니다. 중국 리전 및 에서는 Security Hub CSPM AWS GovCloud (US) Regions이 표준에 대한 예비 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다. Security Hub CSPM은 예비 보안 점수를 생성한 후 24시간마다 점수를 업데이트합니다. 보안 점수가 마지막으로 업데이트된 시점을 확인하려면 Security Hub CSPM이 점수에 대해 제공하는 타임스탬프를 참조할 수 있습니다. 자세한 내용은 보안 점수 계산 단원을 참조하십시오.

표준을 활성화하는 방법은 중앙 구성을 사용하여 여러 계정 및 AWS 리전에서 Security Hub CSPM을 관리하는지 여부에 따라 달라집니다. 다중 계정, 다중 리전 환경에서 표준을 활성화 또는 비활성화하려면 중앙 구성을 사용하는 것을 권장합니다. Security Hub CSPM을와 통합하는 경우 중앙 구성을 사용

할 수 있습니다 AWS Organizations. 중앙 구성을 사용하지 않는 경우, 각 계정 및 각 리전에서 별도로 각 표준을 활성화해야 합니다.

주제


- 여러 계정 및에서 표준 활성화 AWS 리전
- 단일 계정에서 표준 활성화 및 AWS 리전
- 표준의 상태 확인


## 여러 계정 및에서 표준 활성화 AWS 리전

여러 계정에서 보안 표준을 활성화하고 구성하려면 중앙 구성을 AWS 리전사용합니다. 중앙 구성을 사용하면 위임된 Security Hub CSPM 관리자는 하나 이상의 표준을 활성화하는 Security Hub CSPM 구성 정책을 만들 수 있습니다. 그런 다음 관리자는 이 구성 정책을 개별 계정, 조직 단위(OU) 또는 루트와 연결할 수 있습니다. 구성 정책은 집계 영역이라고도 하는 홈 리전과 모든 연결된 리전에 영향을 미칩니다.

구성 정책은 사용자 지정 옵션을 제공합니다. 예를 들어 한 OU에 대해 AWS 기본 보안 모범 사례(FSBP) 표준만 활성화하도록 선택할 수 있습니다. 다른 OU의 경우 FSBP 표준과 Center for Internet Security(CIS) AWS Foundations Benchmark v1.4.0 표준을 모두 활성화하도록 선택할 수 있습니다. 지정한 특정 표준을 활성화하는 구성 정책을 생성하는 방법에 대한 자세한 내용은 구성 정책 생성 및 연결 섹션을 참조하세요.

중앙 구성을 사용하는 경우, Security Hub CSPM은 새로운 계정 또는 기존 계정의 표준을 자동으로 활성화하지 않습니다. 대신, Security Hub CSPM 관리자는 조직의 Security Hub CSPM 구성 정책을 생성할 때 각 계정에서 활성화할 표준을 지정합니다. Security Hub CSPM은 FSBP 표준만 활성화하는 권장 구성 정책을 제공합니다. 자세한 내용은 구성 정책 유형 단원을 참조하십시오.

> **Note**
>
> Security Hub CSPM 관리자는 구성 정책을 사용하여 AWS Control Tower 서비스 관리형 표준을 제외한 모든 표준을 활성화할 수 있습니다. 이 표준을 활성화하려면 관리자가를 AWS Control Tower 직접 사용해야 합니다. 또한 AWS Control Tower 를 사용하여 중앙 관리형 계정에 대해이 표준에서 개별 제어를 활성화하거나 비활성화해야 합니다.

일부 계정이 자기 계정에 대한 표준을 활성화하고 구성하도록 하려면 Security Hub CSPM 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 별도로 표준을 활성화하고 구성해야 합니다.

## 단일 계정에서 표준 활성화 및 AWS 리전

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우, 중앙에서 구성 정책을 사용하여 여러 계정 또는 AWS 리전에서 표준을 활성화할 수 없습니다. 하지만 단일 계정 및 리전에서는 표준을 활성화할 수 있습니다. Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용하여 이 작업을 수행할 수 있습니다.

Security Hub CSPM console

Security Hub CSPM 콘솔을 사용하여 단일 계정 및 리전에서 표준을 활성화하려면 다음 단계를 따르세요.

한 계정과 리전에서 표준을 활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 표준을 활성화하려는 리전을 선택합니다.
3. 탐색 창에서 보안 표준을 선택합니다. 시작 페이지의 보안 표준에 Security Hub CSPM이 현재 지원하는 보안 표준이 나열됩니다. 표준을 이미 활성화한 경우 표준 섹션에는 표준의 현재 보안 점수 및 추가 세부 정보가 포함됩니다.
4. 활성화하려는 표준의 섹션에서 표준 활성화를 선택합니다.

추가 리전에서 표준을 활성화하려면 각각의 추가 리전에서 앞의 단계를 반복합니다.

Security Hub CSPM API

단일 계정 및 리전에서 프로그래밍 방식으로 표준을 활성화하려면 BatchEnableStandards 작업을 사용합니다. 또는 AWS Command Line Interface (AWS CLI)를 사용하는 경우 batch-enable-standards 명령을 실행합니다.

요청에서 `StandardsArn` 파라미터를 사용하여 활성화하려는 표준의 Amazon 리소스 이름(ARN)을 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 예를 들어 다음 명령은 AWS 기본 보안 모범 사례(FSBP) 표준을 활성화합니다.

```
$ 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
```

여기서 *arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0*은 미국 동부(버지니아 북부) 리전에서 FSBP 표준의 ARN이고 *us-east-1*은 이 표준을 활성화할 리전입니다.

표준의 ARN을 가져오려면 DescribeStandards 작업을 사용하거나를 사용하는 경우 describe-standards 명령을 AWS CLI실행합니다.

먼저 계정에서 현재 활성화된 표준의 목록을 검토하려면 GetEnabledStandards 작업을 사용할 수 있습니다. 를 사용하는 경우 get-enabled-standards 명령을 실행하여이 목록을 검색할 AWS CLI수 있습니다.

표준을 활성화하면 Security Hub CSPM은 계정 및 지정된 리전에서 표준을 활성화하는 태스크를 수행하기 시작합니다. 여기에는 표준에 적용되는 모든 제어를 생성하는 태스크가 포함됩니다. 이러한 태스크의 상태를 모니터링하려면 계정 및 리전의 표준 상태를 확인할 수 있습니다.

## 표준의 상태 확인

계정에 대해 보안 표준을 활성화하면 Security Hub CSPM은 계정의 표준에 적용되는 모든 제어를 생성하기 시작합니다. 또한 Security Hub CSPM은 표준의 예비 보안 점수 생성 등 계정의 표준을 활성화하는 추가 태스크를 수행합니다. Security Hub CSPM이 이러한 태스크를 수행하는 동안 계정에서 표준의 상태는 Pending입니다. 그런 다음 표준이 추가 상태를 통과하는데 이를 모니터링 및 확인할 수 있습니다.

> **Note**
>
> 표준의 개별 제어에 대한 변경 사항은 표준의 전체 상태에 영향을 미치지 않습니다. 예를 들어 이전에 비활성화한 제어를 활성화해도 변경 사항은 표준의 상태에 영향을 미치지 않습니다. 마찬가지로, 활성화된 제어의 파라미터 값을 변경해도 변경 사항은 표준의 상태에 영향을 미치지 않습니다.

Security Hub CSPM 콘솔을 사용하여 표준의 상태를 확인하려면 탐색 창에서 보안 표준을 선택합니다. 시작 페이지의 보안 표준에 Security Hub CSPM이 현재 지원하는 보안 표준이 나열됩니다. Security Hub CSPM이 현재 표준을 활성화하는 태스크를 수행하고 있는 경우, 표준 섹션에는 Security Hub CSPM이 여전히 표준의 보안 점수를 생성하고 있는 것으로 나타납니다. 표준이 활성화된 경우 표준 섹션에 현재 점수가 포함됩니다. 결과 보기를 선택하여 표준에 적용되는 개별 제어의 상태를 포함한 추가 세부 정보를 검토합니다. 자세한 내용은 보안 검사 실행 예약 단원을 참조하십시오.

Security Hub CSPM API를 사용하여 프로그래밍 방식으로 표준의 상태를 확인하려면 GetEnabledStandards 작업을 사용합니다. 선택적으로, 요청에서 `StandardsSubscriptionArns` 파라미터를 사용하여 상태를 확인하려는 표준의 Amazon 리소스 이름(ARN)을 지정합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 get-enabled-standards 명령을 실행하여 표준의 상태를 확인할 수 있습니다. 확인할 표준의 ARN을 지정하려면 `standards-subscription-arns` 파라미터를 사용합니다. 지정할 ARN을 확인하려면 DescribeStandards 작업을 사용하거나에 대해 describe-standards 명령을 AWS CLI실행할 수 있습니다.

요청이 성공하면 Security Hub CSPM은 `StandardsSubscription` 객체 배열로 응답합니다. 표준 구독은 계정에 표준이 활성화된 경우 Security Hub CSPM이 계정에 생성하는 AWS 리소스입니다. 각 `StandardsSubscription` 객체는 계정에 대해 현재 활성화되었거나 활성화 또는 비활성화 중인 표준에 대한 세부 정보를 제공합니다. 각 객체에서 `StandardsStatus` 필드는 계정에서 표준의 현재 상태를 나타냅니다.

표준의 상태(`StandardsStatus`)는 다음 중 하나일 수 있습니다.

PENDING

Security Hub CSPM이 현재 계정에 대해 표준을 활성화하는 태스크를 수행하고 있습니다. 여기에는 표준에 적용되는 제어를 생성하는 태스크, 표준의 예비 보안 점수를 생성하는 태스크가 포함됩니다. Security Hub CSPM이 모든 태스크를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 계정에 표준이 이미 활성화되어 있고 Security Hub CSPM이 표준에 새 제어를 추가하고 있는 경우에도 표준이 이 상태일 수 있습니다.

표준이 이 상태에 있는 경우 표준에 적용되는 개별 제어의 세부 정보를 검색하지 못할 수 있습니다. 또한 표준의 개별 제어를 구성하거나 비활성화하지 못할 수 있습니다. 예를 들어 UpdateStandardsControl 작업을 사용하여 제어를 비활성화하려고 하면 오류가 발생합니다.

표준의 개별 제어를 구성하거나 관리할 수 있는지 확인하려면 `StandardsControlsUpdatable` 필드의 값을 참조하세요. 이 필드의 값이 `READY_FOR_UPDATES`인 경우 표준의 개별 제어를 관리하기 시작할 수 있습니다. 그렇지 않으면 Security Hub CSPM이 표준을 활성화하기 위한 추가 처리 태스크를 완료할 때까지 기다려야 합니다.

READY

표준이 현재 계정에 대해 활성화되어 있습니다. Security Hub CSPM은 보안 검사를 실행하고, 표준에 적용되고 현재 활성화된 모든 제어에 대한 조사 결과를 생성할 수 있습니다. 또한 Security Hub CSPM은 각 표준에 대한 보안 점수를 계산합니다.

표준이 이 상태에 있는 경우 표준에 적용되는 개별 제어의 세부 정보를 검색할 수 있습니다. 또한 제어를 구성, 비활성화 또는 다시 활성화할 수 있습니다. 표준을 비활성화할 수도 있습니다.

INCOMPLETE

Security Hub CSPM이 계정에 대해 표준을 완전히 활성화할 수 없었습니다. Security Hub CSPM이 보안 검사를 실행할 수 없고 표준에 적용되고 현재 활성화된 모든 제어에 대한 조사 결과를 생성할 수 없습니다. 또한 Security Hub CSPM은 표준에 대한 보안 점수를 계산할 수 없습니다.

멀티클라우드 표준의 경우 CSPM 커넥터 없이 표준을 활성화`NO_AVAILABLE_MULTICLOUD_CONNECTOR`하면 구독이 상태 이유가 `INCOMPLETE` 로 입력됩니다. 커넥터를 사용할 수 `READY` 있게 되면 구독이 로 자동 전환됩니다.

표준을 완전히 활성화할 수 없는 이유를 확인하려면 `StandardsStatusReason` 배열의 정보를 참조하세요. 이 배열은 Security Hub CSPM이 표준을 활성화하지 못하게 한 문제를 표시합니다. 내부 오류가 발생한 경우 다시 계정에 대해 표준을 활성화해 보세요. 다른 유형의 문제는 AWS Config 설정을 확인하세요. 확인하지 않으려는 개별 제어를 비활성화하거나 표준을 완전히 비활성화할 수도 있습니다.

DELETING

Security Hub CSPM이 현재 계정에서 표준을 비활성화하는 요청을 처리하고 있습니다. 여기에는 표준에 적용되는 제어를 비활성화하는 태스크, 관련 보안 점수를 제거하는 태스크가 포함됩니다. Security Hub CSPM이 요청 처리를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

표준이 이 상태에 있는 경우 계정에 대해 표준을 다시 활성화할 수도 없고 비활성화를 다시 시도할 수도 없습니다. Security Hub CSPM이 먼저 현재 요청의 처리를 완료해야 합니다. 또한 표준에 적용되는 개별 제어의 세부 정보를 검색하거나 제어를 관리할 수 없습니다.

FAILED

Security Hub CSPM이 계정에서 표준을 비활성화할 수 없었습니다. Security Hub CSPM이 표준을 비활성화하려고 할 때 하나 이상의 오류가 발생했습니다. 또한 Security Hub CSPM은 표준에 대한 보안 점수를 계산할 수 없습니다.

표준이 완전히 비활성화되지 않은 이유를 확인하려면 `StandardsStatusReason` 배열의 정보를 참조하세요. 이 배열은 Security Hub CSPM이 표준을 비활성화하지 못하게 한 문제를 표시합니다.

표준이 이 상태에 있는 경우 표준에 적용되는 개별 제어의 세부 정보를 검색하거나 제어를 관리할 수 있습니다. 그러나 계정에 대해 표준을 다시 활성화할 수 있습니다. Security Hub CSPM이 표준을 비활성화하지 못하게 한 문제를 해결하는 경우 표준을 다시 비활성화할 수도 있습니다.

표준의 상태가 `READY`인 경우 Security Hub CSPM은 보안 검사를 실행하고, 표준에 적용되고 현재 활성화된 모든 제어에 대한 조사 결과를 생성합니다. 다른 상태인 경우 Security Hub CSPM은 검사를 실

행하고 활성화된 제어의 전부는 아니지만 일부에 대한 조사 결과를 생성할 수 있습니다. 제어 조사 결과를 생성하거나 업데이트하는 데 최대 24시간이 걸릴 수 있습니다. 자세한 내용은 보안 검사 실행 예약 단원을 참조하십시오.

## 보안 표준 세부 정보 검토

AWS Security Hub CSPM에서 보안 표준을 활성화한 후 콘솔을 사용하여 표준의 세부 정보를 검토할 수 있습니다. 콘솔의 표준 세부 정보 페이지에는 다음 정보가 포함됩니다.

- 표준의 현재 보안 점수.
- 표준에 적용되는 제어 테이블.
- 표준에 적용되는 제어에 대한 집계 통계.
- 표준에 적용되는 제어의 상태에 대한 시각적 요약.
- 활성화되고 표준에 적용되는 제어에 대한 보안 검사의 시각적 요약. 와 통합하면 하나 이상의 조직 계정에서 활성화된 AWS Organizations제어가 활성화된 것으로 간주됩니다.

이러한 세부 정보를 검토하려면 콘솔의 탐색 창에서 보안 표준을 선택합니다. 그런 다음 표준 섹션에서 결과 보기를 선택합니다. 심층 분석을 위해, 데이터를 필터링 및 정렬하고 드릴다운하여 표준에 적용되는 개별 제어의 세부 정보를 검토할 수 있습니다.

주제

- 표준 보안 점수 이해
- 표준의 제어 검토

### 표준 보안 점수 이해

AWS Security Hub CSPM 콘솔의 표준 세부 정보 페이지에는 표준의 보안 점수가 표시됩니다. 이 점수는 표준에 적용되고, 활성화되고, 평가 데이터가 있는 제어의 전체 수에 대한 평가를 통과한 제어의 백분율입니다. 점수 아래에는 표준에 맞게 활성화된 제어에 대한 보안 검사를 요약한 차트가 있습니다. 여기에는 통과 및 실패한 보안 검사의 수가 포함됩니다. 관리자 계정의 경우, 표준 점수와 차트는 관리자 계정 및 모든 구성원 계정에서 집계됩니다. 제어에 대해 있는 실패한 특정 심각도의 보안 검사를 검토하려면 심각도를 선택합니다.

표준을 활성화하면 Security Hub CSPM은 사용자가 Security Hub CSPM 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 표준의 예비 보안 점수를 계산합니다. 점수는 해당 페이지를 방문할 때 활성화된 표준에 대해서만 생성됩니다. 또한 점수를 표시하려면 AWS Config 리소스 기록을 구성해야 합니다. 중국 리전 및 에서는 Security Hub CSPM이 예비 점수를 생성하는 데 최대 24

시간이 걸릴 AWS GovCloud (US) Regions수 있습니다. Security Hub CSPM은 표준의 예비 보안 점수를 생성한 후 24시간마다 점수를 업데이트합니다. 자세한 내용은 보안 점수 계산 단원을 참조하십시오.

보안 표준 세부 정보 페이지의 모든 데이터는 집계 리전을 설정 AWS 리전 하지 않는 한 현재에 고유합니다. 집계 영역을 설정한 경우 보안 점수는 여러 리전에 적용되며 모든 연결된 리전의 조사 결과를 포함합니다. 또한 제어의 규정 준수 상태에는 연결된 리전의 조사 결과가 반영되며, 보안 검사 횟수에는 연결된 리전의 조사 결과가 포함됩니다.

## 표준의 제어 검토

AWS Security Hub CSPM 콘솔을 사용하여 활성화한 표준의 세부 정보를 검토할 때 표준에 적용되는 보안 제어 테이블을 검토할 수 있습니다. 이 테이블에는 각 조사 결과에 대한 다음 정보가 포함되어 있습니다.

- 제어 ID 및 제목.
- 제어 상태. 자세한 내용은 규정 준수 상태 및 제어 상태 평가 단원을 참조하십시오.
- 제어에 할당된 심각도.
- 실패한 검사 수 및 총 검사 수. 해당하는 경우, 실패한 검사 열에는 알 수 없음 상태인 조사 결과의 수도 표시됩니다.
- 제어가 사용자 지정 파라미터를 지원하는지 여부. 자세한 내용은 Security Hub CSPM의 제어 파라미터 이해 단원을 참조하십시오.

Security Hub CSPM은 24시간마다 제어 상태 및 보안 검사 횟수를 업데이트합니다. 페이지 상단의 타임스탬프는 Security Hub CSPM이 가장 최근에 이 데이터를 업데이트한 시점을 나타냅니다.

관리자 계정의 경우, 관리자 계정 및 모든 멤버 계정의 제어 규정 준수 상태 및 보안 검사 횟수가 집계됩니다. 활성화된 제어의 수는 관리자 계정 또는 최소 하나 이상의 멤버 계정에서 표준에 대해 활성화된 제어가 포함됩니다. 비활성화된 제어의 수는 관리자 계정 및 모든 멤버 계정에서 표준에 대해 비활성화된 제어를 포함됩니다.

표준에 적용되는 제어 테이블을 필터링할 수 있습니다. 테이블 옆의 필터링 기준 옵션을 사용하여 표준에 대해 활성화된 제어만 보거나 비활성화된 제어만 볼 수 있습니다. 활성화된 제어만 표시하는 경우, 테이블을 제어 상태별로 추가로 필터링할 수 있습니다. 그러면 특정 제어 상태의 제어에 집중할 수 있습니다. 필터 기준 옵션 외에도 제어 필터링 상자에 필터링 기준을 입력할 수 있습니다. 예를 들어, 제어 ID 또는 제목을 기준으로 필터링할 수 있습니다.

원하는 액세스 방법을 선택합니다. 그런 다음 단계에 따라 활성화한 표준에 적용되는 제어를 검토합니다.

Security Hub CSPM console

활성화된 표준의 제어를 검토하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 보안 표준을 선택합니다.
3. 표준 섹션에서 결과 보기를 선택합니다.

페이지 하단의 테이블에는 표준에 적용되는 모든 제어의 목록이 나열됩니다. 테이블을 필터링하고 정렬할 수 있습니다. 테이블의 현재 페이지를 CSV 파일로 다운로드할 수도 있습니다. 이렇게 하려면 테이블 위에서 다운로드를 선택합니다. 테이블을 필터링한 경우, 다운로드한 파일에는 현재 필터 설정과 일치하는 제어만 포함됩니다.

Security Hub CSPM API

활성화된 표준의 제어를 검토하려면

1. Security Hub CSPM API의 ListSecurityControlDefinitions 작업을 사용합니다. 를 사용하는 경우 list-security-control-definitions 명령을 AWS CLI실행합니다.

   제어를 검토하려는 표준의 Amazon 리소스 이름(ARN)을 지정합니다. 표준의 ARN을 가져오려면 DescribeStandards 작업 또는 describe-standards 명령을 사용합니다. 표준의 ARN을 지정하지 않으면 Security Hub CSPM은 모든 보안 제어 ID를 반환합니다.
2. Security Hub CSPM API의 ListStandardsControlAssociations 작업을 사용하거나 list-standards-control-associations 명령을 실행합니다. 이 작업은 제어가 활성화된 표준을 알려줍니다.

   보안 제어 ID 또는 ARN을 제공하여 제어를 식별합니다. 페이지 매김 파라미터는 선택 사항입니다.

다음 예제에서는 Config.1 제어가 활성화된 표준을 보여줍니다.

```
$ aws securityhub list-standards-control-associations --region us-east-1 --security-control-id Config.1
```

# 자동으로 활성화되는 보안 표준 끄기

조직이 중앙 구성을 사용하지 않는 경우 로컬 구성이라는 구성 유형을 사용합니다. 로컬 구성을 사용하면 AWS Security Hub CSPM은 멤버 계정이 조직에 가입할 때 새로운 멤버 계정의 기본 보안 표준을 자동으로 활성화할 수 있습니다. 이러한 기본 표준에 적용되는 모든 제어도 자동으로 활성화됩니다.

현재 기본 보안 표준은 AWS Foundational Security Best Practices 표준과 Center for Internet Security(CIS) AWS Foundations Benchmark v1.2.0 표준입니다. 이러한 표준에 대한 자세한 내용은 Security Hub CSPM용 표준 참조 섹션을 참조하세요.

새 멤버 계정에 대한 보안 표준을 수동으로 활성화하려는 경우 기본 표준의 자동 활성화를 끌 수 있습니다. 와 통합 AWS Organizations 하고 로컬 구성을 사용하는 경우에만이 작업을 수행할 수 있습니다. 중앙 구성을 사용하는 경우, 대신 기본 표준을 활성화하는 구성 정책을 만들고 정책을 루트에 연결할 수 있습니다. 다른 정책과 연결하거나 자체 관리하지 않는 한 모든 조직 계정 및 OU는 이 구성 정책을 상속합니다. 와 통합하지 않으면 Security Hub CSPM 이상을 처음 활성화 AWS Organizations할 때 기본 표준을 비활성화할 수 있습니다. 자세한 방법은 표준 비활성화을 참조하세요.

새 멤버 계정에 대한 기본 표준 자동 활성화를 끄려면 Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용할 수 있습니다.

Security Hub CSPM console

Security Hub CSPM 콘솔을 사용하여 기본 표준 자동 활성화를 끄려면 다음 단계를 따르세요.

기본 표준 자동 활성화를 끄려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.

   관리자 계정의 보안 인증을 사용하여 로그인합니다.
2. 탐색 창의 설정에서 구성을 선택합니다.
3. 개요 섹션에서 편집을 선택합니다.
4. 새 계정 설정에서 기본 보안 표준 활성화 확인란을 선택 해제합니다.
5. 확인을 선택합니다.

Security Hub CSPM API

프로그래밍 방식으로 기본 표준 자동 활성화를 끄려면 Security Hub CSPM 관리자 계정에서 Security Hub CSPM API의 UpdateOrganizationConfiguration 작업을 사용합니다. 요청에서 `AutoEnableStandards` 파라미터에 `NONE`을 지정합니다.

를 사용하는 경우 update-organization-configuration 명령을 AWS CLI실행하여 기본 표준의 자동 활성화를 끕니다. `auto-enable-standards` 파라미터에서 `NONE`를 지정합니다. 예를 들어 다음 명령은 새 멤버 계정에 대해 Security Hub CSPM을 자동으로 활성화하고 기본 표준 자동 활성화를 끕니다.

```
$ aws securityhub update-organization-configuration --auto-enable --auto-enable-standards NONE
```

## 보안 표준 비활성화

AWS Security Hub CSPM에서 보안 표준을 비활성화하면 다음이 발생합니다.

- 현재 활성화된 다른 표준과 연결되지 않은 한, 표준에 적용되는 모든 제어가 비활성화됩니다.
- 비활성화된 제어에 대한 보안 검사는 더 이상 실행되지 않으며 비활성화된 제어에 대한 추가 조사 결과는 생성되지 않습니다.
- 비활성화된 제어에 대한 기존 조사 결과는 약 3~5일 후에 자동으로 보관됩니다.
- AWS Config 비활성화된 컨트롤에 대해 Security Hub CSPM이 생성한 규칙이 삭제됩니다.

적절한 AWS Config 규칙의 삭제는 일반적으로 표준을 비활성화한 후 몇 분 이내에 이루어집니다. 하지만 시간이 더 걸릴 수도 있습니다. 첫 번째 요청에서 규칙 삭제가 실패하면 Security Hub CSPM은 12시간마다 재시도합니다. 하지만 Security Hub CSPM을 비활성화했거나 활성화한 다른 표준이 없는 경우, Security Hub CSPM이 다시 시도할 수 없습니다. 즉, 규칙을 삭제할 수 없습니다. 이 경우 규칙을 삭제해야 하는 경우에 문의하십시오 AWS Support.

주제

- 여러 계정 및에서 표준 비활성화 AWS 리전
- 단일 계정 및에서 표준 비활성화 AWS 리전

### 여러 계정 및에서 표준 비활성화 AWS 리전

여러 계정에서 보안 표준을 비활성화하려면 중앙 구성을 AWS 리전사용합니다. 중앙 구성을 사용하면 위임된 Security Hub CSPM 관리자는 하나 이상의 표준을 비활성화하는 Security Hub CSPM 구성 정책을 만들 수 있습니다. 그런 다음 관리자는 이 구성 정책을 개별 계정, 조직 단위(OU) 또는 루트와 연결할 수 있습니다. 구성 정책은 집계 영역이라고도 하는 홈 리전과 모든 연결된 리전에 영향을 미칩니다.

구성 정책은 사용자 지정 옵션을 제공합니다. 예를 들어 한 OU에서 PCI DSS(지불 카드 산업 데이터 보안 표준)를 비활성화하도록 선택할 수 있습니다. 다른 OU에서는 PCI DSS 및 NIST(국립 표준 기술 연구소) SP 800-53 개정 5 표준을 모두 비활성화하도록 선택할 수 있습니다. 지정한 개별 표준을 활성화 또는 비활성화하는 구성 정책을 생성하는 방법에 대한 자세한 내용은 구성 정책 생성 및 연결 섹션을 참조하세요.

> **Note**
>
> Security Hub CSPM 관리자는 구성 정책을 사용하여 AWS Control Tower 서비스 관리형 표준을 제외한 모든 표준을 비활성화할 수 있습니다. 이 표준을 비활성화하려면 관리자가를 AWS Control Tower 직접 사용해야 합니다. 또한 AWS Control Tower 를 사용하여 중앙 관리형 계정에 대해이 표준에서 개별 제어를 비활성화하거나 활성화해야 합니다.

일부 계정이 자기 계정에 대한 표준을 구성하거나 비활성화하도록 하려면 Security Hub CSPM 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 개별적으로 표준을 비활성화해야 합니다.

## 단일 계정 및에서 표준 비활성화 AWS 리전

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우, 중앙에서 구성 정책을 사용하여 여러 계정 또는 AWS 리전에서 표준을 비활성화할 수 없습니다. 하지만 단일 계정 및 리전에서는 표준을 비활성화할 수 있습니다. Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용하여 이 작업을 수행할 수 있습니다.

Security Hub CSPM console

Security Hub CSPM 콘솔을 사용하여 단일 계정 및 리전에서 표준을 비활성화하려면 다음 단계를 따르세요.

한 계정 및 리전에서 표준을 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 표준을 비활성화하려는 리전을 선택합니다.
3. 탐색 창에서 보안 표준을 선택합니다.
4. 비활성화하려는 표준의 섹션에서 표준 비활성화를 선택합니다.

추가 리전에서 표준을 비활성화하려면, 각 추가 리전에서 이전 단계를 반복합니다.

Security Hub CSPM API

단일 계정 및 리전에서 프로그래밍 방식으로 표준을 비활성화하려면 BatchDisableStandards 작업을 사용합니다. 또는 AWS Command Line Interface (AWS CLI)를 사용하는 경우 batch-disable-standards 명령을 실행합니다.

요청에서 `StandardsSubscriptionArns` 파라미터를 사용하여 비활성화하려는 표준의 Amazon 리소스 이름(ARN)을 지정합니다. 를 사용하는 경우 `standards-subscription-arns` 파라미터를 AWS CLI사용하여 ARN을 지정합니다. 또한 요청이 적용되는 리전을 지정합니다. 예를 들어 다음 명령은 계정(*123456789012*)에 대한 AWS 기본 보안 모범 사례(FSBP) 표준을 비활성화합니다.

```
$ 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
```

여기서 *arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0*은 미국 동부(버지니아 북부) 리전에서 FSBP 표준의 ARN이고 *us-east-1*은 이 표준을 비활성화할 리전입니다.

표준의 ARN을 가져오려면 GetEnabledStandards 작업을 사용할 수 있습니다. 이 작업은 계정에서 현재 활성화된 표준에 대한 정보를 검색합니다. 를 사용하는 경우 get-enabled-standards 명령을 실행하여이 정보를 검색할 AWS CLI수 있습니다.

표준을 비활성화하면 Security Hub CSPM은 계정 및 지정된 리전에서 표준을 비활성화하는 태스크를 수행하기 시작합니다. 여기에는 표준에 적용되는 모든 제어를 비활성화하는 태스크가 포함됩니다. 이러한 태스크의 상태를 모니터링하려면 계정 및 리전의 표준 상태를 확인할 수 있습니다.

## Security Hub CSPM의 보안 제어 이해

AWS Security Hub CSPM에서 제어라고도 하는 보안 제어는 조직이 정보의 기밀성, 무결성 및 가용성을 보호하는 데 도움이 되는 보안 표준 내의 보호 장치입니다. Security Hub CSPM에서 제어는 특정 AWS 리소스와 관련이 있습니다.

하나 이상의 표준에서 제어를 활성화하면 Security Hub CSPM이 해당 표준에 대한 보안 검사를 실행하기 시작합니다. 보안 검사는 Security Hub CSPM 조사 결과를 생성합니다. 제어를 비활성화하면

Security Hub CSPM이 해당 제어에 대한 보안 검사 실행을 중지하고 조사 결과가 더 이상 생성되지 않습니다.

단일 계정 및에 대해 개별적으로 제어를 활성화하거나 비활성화할 수 있습니다 AWS 리전. 다중 계정 환경에서 시간을 절약하고 구성 드리프트를 줄이려면 중앙 구성을 사용하여 제어를 활성화하거나 비활성화하는 것이 좋습니다. 중앙 구성을 사용하면 위임된 Security Hub CSPM 관리자가 여러 계정 및 리전에서 제어를 구성하는 방법을 지정하는 정책을 생성할 수 있습니다. 표준 전반의 제어 기능 활성화 및 비활성화에 대한 자세한 내용은 Security Hub CSPM에서 제어 활성화 섹션을 참조하세요.

## 통합 제어 보기

Security Hub CSPM 콘솔의 제어 페이지에는 현재에서 사용할 수 있는 모든 제어가 표시됩니다 AWS 리전 (보안 표준 페이지를 방문하여 활성화된 표준을 선택하여 표준의 컨텍스트에서 제어를 볼 수 있음). Security Hub CSPM은 표준 전체에 걸쳐 일관된 보안 제어 ID, 제목 및 설명을 제어에 할당합니다. 제어 IDs에는 관련 AWS 서비스 및 고유 번호(예: CodeBuild.3).가 포함됩니다.

Security Hub CSPM 콘솔의 제어 페이지에서 다음 정보를 사용할 수 있습니다.

- 데이터가 포함된 활성화된 총 제어 수와 비교하여 통과된 제어의 비율을 기준으로 한 전체 보안 점수
- 지원되는 모든 Security Hub CSPM 제어의 제어 상태 분석
- 통과 및 실패한 총 보안 검사 수입니다.
- 심각도가 다양한 제어를 위한 실패한 보안 검사 수와 실패한 검사에 대한 자세한 내용을 볼 수 있는 링크입니다.
- Security Hub CSPM 제어 목록으로, 특정 제어 하위 집합을 볼 수 있는 필터가 있습니다.

제어 페이지에서 제어를 선택하여 세부 정보를 보고 제어에서 생성된 조사 결과에 대해 조치를 취할 수 있습니다. 이 페이지에서 현재 AWS 계정 및에서 보안 제어를 활성화하거나 비활성화할 수도 있습니다 AWS 리전. 제어 페이지의 활성화 및 비활성화 조치는 모든 표준에 적용됩니다. 자세한 내용은 Security Hub CSPM에서 제어 활성화 섹션을 참조하세요.

관리자 계정의 경우, 제어 페이지에는 구성원 계정 전체의 제어 상태가 반영됩니다. 하나 이상의 멤버 계정에서 제어 확인에 실패하면 제어 상태는 실패입니다. 집계 리전을 설정한 경우, 제어 페이지에는 연결된 모든 리전의 제어 상태가 반영됩니다. 연결된 리전 하나 이상에서 제어 확인에 실패하면 제어 상태는 실패입니다.

통합 제어 보기는 워크플로에 영향을 미칠 수 있는 AWS Security Finding Format(ASFF)의 제어 결과 필드를 변경합니다. 자세한 내용은 통합 제어 보기 - ASFF 변경 단원을 참조하십시오.

## 제어에 대한 요약 보안 점수

제어 페이지에는 0~ 100%의 요약 보안 점수가 표시됩니다. 요약 보안 점수는 표준 전체의 데이터를 사용하여 활성화된 제어의 총 수와 비교한 통과된 제어의 비율을 기준으로 계산됩니다.

> **Note**
>
> 제어에 대한 전체 보안 점수를 보려면 Security Hub CSPM에 액세스하는 데 사용하는 IAM 역할에 **`BatchGetControlEvaluations`**를 직접적으로 호출할 수 있는 권한을 추가해야 합니다. 특정 표준의 보안 점수를 보는 데는 이 권한이 필요하지 않습니다.

Security Hub CSPM을 활성화하면 Security Hub CSPM은 사용자가 Security Hub CSPM 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 초기 보안 점수를 계산합니다. 중국 리전 및 AWS GovCloud (US) Regions에 처음으로 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

전체 보안 점수 외에도 Security Hub CSPM은 사용자가 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 각 활성화된 표준에 대한 표준 보안 점수를 계산합니다. 현재 활성화된 표준 목록을 보려면 `GetEnabledStandards` API 작업을 사용하세요.

AWS Config 점수를 표시하려면 리소스 기록으로를 활성화해야 합니다. Security Hub CSPM이 보안 점수를 계산하는 방법에 대한 자세한 내용은 보안 점수 계산 섹션을 참조하세요.

Security Hub CSPM은 점수를 처음 생성한 후 24시간마다 보안 점수를 업데이트합니다. Security Hub CSPM은 보안 점수가 마지막으로 업데이트된 시점을 나타내는 타임스탬프를 표시합니다.

집계 리전을 설정한 경우, 전체 보안 점수는 연결된 리전 전반의 제어 조사 결과를 반영합니다.

## Security Hub CSPM 제어 참조

이 제어 참조는 사용 가능한 AWS Security Hub CSPM 제어 표와 각 제어에 대한 자세한 정보 링크를 제공합니다. 이 테이블에서 제어는 제어 ID를 기준으로 알파벳 순으로 나열되어 있습니다. Security Hub CSPM에서 사용 중인 제어만 여기에 포함됩니다. 사용 중지된 제어는 이 테이블에서 제외됩니다.

이 테이블은 각 제어에 대해 다음 정보가 표시됩니다.

- 보안 제어 ID -이 ID는 표준에 적용되며 제어와 관련된 AWS 서비스 및 리소스를 나타냅니다. Security Hub CSPM 콘솔은 계정에서 통합 제어 조사 결과가 켜져 있는지 또는 사용 중지되었는지에 관계없이 보안 제어 ID를 표시합니다. 하지만 Security Hub CSPM 조사 결과는 계정에 통합 제어 조

사 결과가 설정된 경우에만 보안 제어 ID를 참조합니다. 계정에서 통합 제어 조사 결과가 해제된 경우, 일부 제어 ID는 제어 조사 결과의 표준에 따라 다릅니다. 표준별 제어 ID를 보안 제어 ID에 매핑하는 방법은 통합이 제어 ID 및 제목에 미치는 영향 섹션을 참조하세요.

보안 제어를 위한 자동화를 설정하려는 경우, 제목이나 설명보다는 제어 ID를 기준으로 필터링하는 것이 좋습니다. Security Hub CSPM은 때때로 제어의 제목이나 설명을 업데이트할 수 있지만 제어 ID는 동일하게 유지됩니다.

제어 ID는 숫자를 건너뛸 수 있습니다. 이는 향후 제어를 위한 자리표시자입니다.

- 보안 제어 제목 - 이 제목은 여러 표준에 적용됩니다. Security Hub CSPM 콘솔에는 계정에서 통합 제어 조사 결과가 켜져 있는지 또는 사용 중지되었는지에 관계없이 보안 제어 제목이 표시됩니다. 그러나 Security Hub CSPM 조사 결과는 계정에 통합 제어 조사 결과가 설정된 경우에만 보안 제어 제목을 참조합니다. 계정에서 통합 제어 조사 결과가 해제된 경우, 일부 제어 목록은 제어 조사 결과의 표준에 따라 다릅니다. 표준별 제어 ID를 보안 제어 ID에 매핑하는 방법은 통합이 제어 ID 및 제목에 미치는 영향 섹션을 참조하세요.
- 적용 가능한 표준 - 제어가 적용되는 표준을 나타냅니다. 제어를 선택하면 서드 파티 규정 준수 프레임워크의 특정 요구 사항을 검토할 수 있습니다.
- 심각도 - 제어의 심각도는 보안 관점에서 그 중요성을 식별합니다. Security Hub CSPM에서 제어 심각도를 결정하는 방법에 대한 자세한 내용은 제어 조사 결과의 심각도 수준 섹션을 참조하세요.
- 사용자 지정 파라미터 지원 - 제어가 하나 이상의 파라미터에 대한 사용자 지정 값을 지원하는지 여부를 나타냅니다. 제어를 선택하면 파라미터 세부 정보를 검토할 수 있습니다. 자세한 내용은 Security Hub CSPM의 제어 파라미터 이해 단원을 참조하십시오.
- 일정 유형 - 제어가 평가되는 시기를 나타냅니다. 자세한 내용은 보안 검사 실행 예약 단원을 참조하십시오.

제어를 선택하면 추가 세부 정보를 검토할 수 있습니다. 제어는 보안 제어 ID를 기준으로 알파벳 순으로 나열되어 있습니다.

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Account.1 | 에 대한 보안 연락처 정보를 제공해야 합니다. AWS 계정 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| | | 션 벤치마크 v3.0.0, AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | | | |
| Account.2 | AWS 계정 는 AWS Organizations 조직의 일부여야 합니다. | NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 주기적 |
| ACM.1 | 가져온 인증서 및 ACM 발행 인증서는 지정된 기간 후 갱신해야 합니다 | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊙ 예 | 변경이 트리거되고 주기적입니다. |
| ACM.2 | ACM에서 관리하는 RSA 인증서는 2,048 비트 이상의 키 길이를 사용해야 합니다 | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| ACM.3 | ACM 인증서에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Amplify.1 | Amplify 앱에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Amplify.2 | Amplify 브랜치에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| APIGateway.1 | API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| APIGateway.2 | API Gateway REST API 단계는 백엔드 인증에 SSL 인증서를 사용하도록 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| APIGateway.3 | API Gateway REST API 단계에는 AWS X-Ray 추적이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| APIGateway.4 | API Gateway는 WAF 웹 ACL과 연결되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| APIGateway.5 | API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| APIGateway.8 | API Gateway 경로에는 권한 부여 유형을 지정해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |
| APIGateway.9 | API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| APIGateway.10 | API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| APIGateway.11 | API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| AppConfig.1 | AWS AppConfig 애플리케이션에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| AppConfig.2 | AWS AppConfig 구성 프로필에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| AppConfig.3 | AWS AppConfig 환경에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| AppConfig.4 | AWS AppConfig 확장 연결에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| AppFlow.1 | Amazon AppFlow 흐름에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| AppRunner.1 | App Runner 서비스에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| AppRunner.2 | App Runner VPC 커넥터에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| AppSync.2 | AWS AppSync에는 필드 수준 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v4.0.1 | 중간 | ✓ 예 | 변경이 트리거됨 |
| AppSync.4 | AWS AppSync GraphQL APIs 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| AppSync.5 | AWS AppSync GraphQL APIs API 키로 인증해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| Athena.2 | Athena 데이터 카탈로그에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Athena.3 | Athena 작업 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Athena.4 | Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| AutoScaling.1 | 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 낮음 | ✗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| AutoScaling.2 | Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포함해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 변경이 트리거됨 |
| AutoScaling.3 | Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| Autoscaling.5 | Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| AutoScaling.6 | Auto Scaling 그룹은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| AutoScaling.9 | EC2 Auto Scaling 그룹은 EC2 시작 템플릿을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| AutoScaling.10 | EC2 Auto Scaling 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Backup.1 | AWS Backup 복구 시점은 저장 시 암호화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Backup.2 | AWS Backup 복구 시점에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Backup.3 | AWS Backup 볼트에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Backup.4 | AWS Backup 보고서 계획에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Backup.5 | AWS Backup 백업 계획에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Batch.1 | Batch 작업 대기열에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Batch.2 | Batch 예약 정책에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Batch.3 | Batch 컴퓨팅 환경에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Batch.4 | 관리형 Batch 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Bedrock.1 | Amazon Bedrock 데이터 소스는 고객 관리형 AWS KMS 키로 암호화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| BedrockAgentCore.1 | Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| BedrockAgentCore.2 | Bedrock AgentCore Gateways는 인바운드 요청에 대한 승인이 필요합니다. | AWS 기본 보안 모범 사례 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| BedrockAgentCore.3 | Bedrock AgentCore 메모리는 고객 관리형 AWS KMS 키로 암호화해야 합니다. | NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| BedrockAgentCore.4 | Bedrock AgentCore Gateway는 고객 관리형 AWS KMS 키로 암호화해야 합니다. | NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| BedrockAgentCore.5 | Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| BedrockAgentCore.6 | Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| BedrockAgentCore.7 | Bedrock AgentCore 사용자 지정 코드 인터프리터는 프라이빗 네트워크 구성을 사용해야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFormation.2 | CloudFormation 스택에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| CloudFormation.3 | CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFormation.4 | CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudFront.1 | CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.3 | CloudFront 배포는 전송 중 암호화가 필요합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.4 | CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.5 | CloudFront 배포에는 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.6 | CloudFront 배포에는 WAF가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.7 | CloudFront 배포에는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.8 | CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudFront.9 | CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.10 | CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.12 | CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| CloudFront.13 | CloudFront 배포에서는 오리진 액세스 제어를 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.14 | CloudFront 배포에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| CloudFront.15 | CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudFront.16 | CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudFront.17 | CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CloudTrail.1 | CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 주기적 |
| CloudTrail.2 | CloudTrail에서 유휴 시 암호화를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.2.0, CIS AWS 파운데이션 벤치마크 v1.4.0 AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v3.2.1, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudTrail.3 | 하나 이상의 CloudTrail 추적을 활성화해야 합니다. | NIST SP 800-171 개정 2, PCI DSS v4.0.1, PCI DSS v3.2.1 | 높음 | ⊗ 아니요 | 주기적 |
| CloudTrail.4 | CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1, PCI DSS v3.2.1 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudTrail.5 | CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, CIS AWS 파운데이션 벤치마크 v1.4.0, AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudTrail.6 | CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, CIS AWS 파운데이션 벤치마크 v1.4.0, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거되고 주기적입니다. |
| CloudTrail.7 | CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.2.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v3.0.0, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudTrail.9 | CloudTrail 추적에는 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| CloudTrail.10 | CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화해야 합니다. AWS KMS keys | NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudWatch.1 | 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2, PCI DSS v3.2.1 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.2 | 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.3 | MFA 없는 로그인에 대해 관리 콘솔에 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.4 | IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.5 | CloudTrail 구성 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudWatch.6 | AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.7 | 고객 생성 CMK 활성화 또는 예약된 삭제에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.8 | S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.9 | AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.10 | 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudWatch.11 | 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.12 | 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.13 | 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.14 | VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 주기적 |
| CloudWatch.15 | CloudWatch 경보에는 지정된 작업이 구성되어 있어야 합니다. | NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 높음 | ⊙ 예 | 변경이 트리거됨 |
| CloudWatch.16 | CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다. | NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CloudWatch.17 | CloudWatch 경보 조치를 활성화해야 합니다. | NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| CodeArtifact.1 | CodeArtifact 리포지토리에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| CodeBuild.1 | CodeBuild Bitbucket 소스 리포지토리 URL에 민감한 자격 증명 정보가 포함되어서는 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| CodeBuild.2 | CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| CodeBuild.3 | CodeBuild S3 로그는 암호화되어야 합니다 | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1, | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| CodeBuild.4 | CodeBuild 프로젝트 환경에는 로깅 구성이 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| CodeBuild.7 | CodeBuild 보고서 그룹 내보내기는 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| CodeGuruProfiler.1 | CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| CodeGuruReviewer.1 | CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Cognito.1 | Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✓ 예 | 변경이 트리거됨 |
| Cognito.2 | Cognito ID 풀은 인증되지 않은 ID를 허용해서는 안 됩니다. | AWS 기본 보안 모범 사례 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| Cognito.3 | Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✓ 예 | 변경이 트리거됨 |
| Cognito.4 | Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| Cognito.5 | Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Cognito.6 | Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Config.1 | AWS Config 를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1 | 심각 | ⊙ 예 | 주기적 |
| Connect.1 | Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Connect.2 | Connect Customer 인스턴스에는 CloudWatch 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DataFirehose.1 | Firehose 전송 스트림은 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| DataSync.1 | DataSync 작업에는 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DataSync.2 | DataSync 태스크에는 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Detective.1 | 탐지 동작 그래프에는 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| DMS.1 | Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 주기적 |
| DMS.2 | DMS 인증서에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| DMS.3 | DMS 이벤트 구독에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| DMS.4 | DMS 복제 인스턴스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| DMS.5 | DMS 복제 서브넷 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| DMS.6 | DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DMS.7 | 대상 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DMS.8 | 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DMS.9 | DMS 엔드포인트는 SSL을 사용해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DMS.10 | Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DMS.11 | MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| DMS.12 | Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DMS.13 | DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DocumentDB.1 | Amazon DocumentDB 클러스터는 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DocumentDB.2 | Amazon DocumentDB 클러스터는 적절한 백업 보존 기간을 가져야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ✓ 예 | 변경이 트리거됨 |
| DocumentDB.3 | Amazon DocumentDB 수동 클러스터 스냅샷은 퍼블릭이 아니어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| DocumentDB.4 | Amazon DocumentDB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DocumentDB.5 | Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| DocumentDB.6 | Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| DynamoDB.1 | DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |
| DynamoDB.2 | DynamoDB 테이블에는 특정 시점 복구가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| DynamoDB.3 | DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| DynamoDB.4 | DynamoDB 테이블은 백업 계획에 있어야 합니다. | NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |
| DynamoDB.5 | DynamoDB 테이블에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| DynamoDB.6 | DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| DynamoDB 7 | DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| EC2.1 | EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 심각 | ⊗ 아니요 | 주기적 |
| EC2.2 | VPC 기본 보안 그룹은 인바운드 또는 아웃바운드 트래픽을 허용하지 않아야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, CIS AWS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.3 | 연결된 EBS 볼륨은 저장 시 암호화되어야 되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.4 | 중지된 EC2 인스턴스는 지정된 기간 후에 제거해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.6 | VPC 흐름 로깅은 모든 VPC에서 활성화되어야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, CIS AWS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 주기적 |
| EC2.7 | EBS 기본 암호화를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, AWS 기본 보안 모범 사례 v1.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| EC2.8 | EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.9 | EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.10 | Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 주기적 |
| EC2.12 | 사용하지 않는 EC2 EIP를 제거해야 합니다. | PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.13 | 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 높음 | ⊗ 아니요 | 변경이 트리거되고 주기적입니다. |
| EC2.14 | 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거되고 주기적입니다. |
| EC2.15 | EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1, | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.16 | 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1, | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.17 | EC2 인스턴스는 ENI를 여러 개 사용해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.18 | 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 높음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.19 | 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 심각 | ⊗ 아니요 | 변경이 트리거되고 주기적입니다. |
| EC2.20 | AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.21 | 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.22 | 사용되지 않는 EC2 보안 그룹은 제거해야 합니다. | | 중간 | ⊗ 아니요 | 주기적 |
| EC2.23 | EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.24 | EC2 반가상화 인스턴스 유형은 사용할 수 없습니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.25 | EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.28 | EBS 볼륨은 백업 계획에 포함되어야 합니다. | NIST SP 800-53 개정 5 | 낮음 | ⊙ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.33 | EC2 transit Gateway Attachment에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.34 | EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.35 | EC2 네트워크 인터페이스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.36 | EC2 고객 게이트웨이에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.37 | EC2 Elastic IP 주소에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.38 | EC2 인스턴스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.39 | EC2 인터넷 게이트웨이에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.40 | EC2 NAT 게이트웨이에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.41 | EC2 네트워크 ACL에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.42 | EC2 라우팅 테이블에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.43 | EC2 보안 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.44 | EC2 서브넷에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.45 | EC2 볼륨에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.46 | Amazon VPC에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.47 | Amazon VPC 엔드포인트 서비스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.48 | Amazon VPC 플로우 로그에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.49 | Amazon VPC 피어링 연결에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EC2.50 | EC2 VPN 게이트웨이에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.51 | EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.52 | EC2 전송 게이트웨이에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.53 | EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| EC2.54 | EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| EC2.55 | VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |
| EC2.56 | VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.57 | VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 주기적 |
| EC2.58 | VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 주기적 |
| EC2.60 | VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 주기적 |
| EC2.170 | EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 낮음 | ✗ 아니요 | 변경이 트리거됨 |
| EC2.171 | EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| EC2.172 | EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.173 | 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.174 | EC2 DHCP 옵션 세트에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.175 | EC2 시작 템플릿에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.176 | EC2 접두사 목록에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.177 | EC2 트래픽 미러 세션에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.178 | EC2 트래픽 미러 필터에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.179 | EC2 트래픽 미러 대상에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| EC2.180 | EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EC2.181 | EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.182 | EBS 스냅샷은 공개적으로 액세스할 수 없어야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| EC2.183 | EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECR.1 | ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| ECR.2 | ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECR.3 | ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECR.4 | ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ECR.5 | ECR 리포지토리는 고객 관리형 AWS KMS keys로 암호화해야 합니다. | NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 변경이 트리거됨 |
| ECS.2 | ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| ECS.3 | ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| ECS.4 | ECS 컨테이너는 권한이 없는 상태로 실행되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| ECS.5 | ECS 컨테이너는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| EC.8 | 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| ECS.9 | ECS 작업 정의에는 로깅 구성이 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ✗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ECS.10 | ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECS.12 | ECS 클러스터는 Container Insights를 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECS.13 | ECS 서비스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| ECS.14 | ECS 클러스터에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| ECS.15 | ECS 작업 정의에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| ECS.16 | ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| ECS.17 | ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다. | NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECS.18 | ECS 작업 정의는 EFS 볼륨에 전송 중 암호화를 사용해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECS.19 | ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ECS.20 | ECS 작업 정의는 Linux 컨테이너 정의에서 루트가 아닌 사용자를 구성해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ECS.21 | ECS 작업 정의는 Windows 컨테이너 정의에서 관리자가 아닌 사용자를 구성해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EFS.1 | 를 사용하여 유휴 파일 데이터를 암호화하도록 Elastic File System을 구성해야 합니다. AWS KMS | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| EFS.2 | Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| EFS.3 | EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EFS.4 | EFS 액세스 포인트는 사용자 ID를 적용해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EFS.5 | EFS 액세스 포인트에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EFS.6 | EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다. | NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 주기적 |
| EFS.7 | EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| EFS.8 | EFS 파일 시스템은 저장 시 암호화해야 합니다. | CIS AWS Foundations Benchmark v5.0.0, AWS 기본 보안 모범 사례 | 중간 | ✓ 예 | 변경이 트리거됨 |
| EKS.1 | EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✗ 아니요 | 주기적 |
| EKS.2 | EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| EKS.3 | EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EKS.6 | EKS 클러스터에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EKS.7 | EKS ID 제공업체 구성에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EKS.8 | EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| EKS.9 | EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ✗ 아니요 | 변경이 트리거됨 |
| ElastiCache.1 | ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ✓ 예 | 주기적 |
| ElastiCache.2 | ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✗ 아니요 | 주기적 |
| ElastiCache.3 | ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ElastiCache.4 | ElastiCache 복제 그룹은 저장 시 암호화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| ElastiCache.5 | ElastiCache 복제 그룹은 전송 중 암호화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| ElastiCache.6 | 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis AUTH가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| ElastiCache.7 | ElastiCache 클러스터에서는 기본 서브넷 그룹을 사용하지 않아야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 주기적 |
| ElasticBeanstalk.1 | Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| ElasticBeanstalk.2 | Elastic Beanstalk 관리형 플랫폼 업데이트를 활성화해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ✓ 예 | 변경이 트리거됨 |
| ElasticBeanstalk.3 | Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ELB.1 | Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| ELB.2 | SSL/HTTPS 리스너가 있는 Classic Load Balancer는 AWS Certificate Manager에서 제공하는 인증서를 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.3 | Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.4 | http 헤더를 삭제하도록 Application Load Balancer를 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.5 | Application 및 Classic Load Balancer 로깅이 활성화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.6 | 애플리케이션, 게이트웨이, Network Load Balancers에는 삭제 보호가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ELB.7 | Classic Load Balancer connection draining 레이닝이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.8 | SSL 리스너가 있는 Classic Load Balancer는 강력한 구성이 있는 사전 정의된 보안 정책을 사용해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.9 | Classic Load Balancer에서 교차 영역 로드 밸런싱을 사용 설정해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.10 | Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 변경이 트리거됨 |
| ELB.12 | Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기 완화 모드로 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.13 | 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ELB.14 | Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.16 | Application Load Balancer는 AWS WAF 웹 ACL과 연결되어야 합니다. | NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.17 | 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.18 | Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ELB.21 | Application 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ELB.22 | ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EMR.1 | Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| EMR.2 | Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 주기적 |
| EMR.3 | Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| EMR.4 | Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ES.1 | Elasticsearch 도메인에서 저장 시 암호화를 활성화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| ES.2 | Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v3.2.1, PCI DSS v4.0.1, NIST SP 800-53 개정 5 | 심각 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| ES.3 | Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1, | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ES.4 | CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅을 활성화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ES.5 | Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ES.6 | ElasticSearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ES.7 | Elasticsearch 도메인은 최소 세 개의 전용 마스터 노드로 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ES.8 | Elasticsearch 도메인에 대한 연결은 TLS 보안 정책을 사용하여 암호화해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| ES.9 | Elasticsearch 도메인에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| EventBridge.2 | EventBridge 이벤트 버스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| EventBridge.3 | EventBridge 사용자 지정 이벤트 버스에 리소스 기반 정책이 연결되어 있어야 합니다 | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 낮음 | ✗ 아니요 | 변경이 트리거됨 |
| EventBridge.4 | EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다. | NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| FraudDetector.1 | Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| FraudDetector.2 | Amazon Fraud Detector 레이블에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| FraudDetector.3 | Amazon Fraud Detector 결과에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| FraudDetector.4 | Amazon Fraud Detector 변수에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| FSx.1 | FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 주기적 |
| FSx.2 | FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 주기적 |
| FSx.3 | FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| FSx.4 | FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊙ 예 | 주기적 |
| FSx.5 | FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| Glue.1 | AWS Glue 작업에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Glue.3 | AWS Glue 기계 학습 변환은 저장 시 암호화되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Glue.4 | AWS Glue Spark 작업은의 지원되는 버전에서 실행되어야 합니다. AWS Glue | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| GlobalAccelerator.1 | Global Accelerator 액셀러레이터에는 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| GuardDuty.1 | GuardDuty를 활성화해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v3.2.1, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| GuardDuty.2 | GuardDuty 필터에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| GuardDuty.3 | GuardDuty IPSet에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| GuardDuty.4 | GuardDuty 탐지기에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| GuardDuty.5 | GuardDuty EKS Audit Log Monitoring을 활성화해야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 주기적 |
| GuardDuty.6 | GuardDuty Lambda 보호를 활성화해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| GuardDuty.7 | GuardDuty EKS 런타임 모니터링을 활성화해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| GuardDuty.8 | EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 주기적 |
| GuardDuty.9 | GuardDuty RDS 보호가 활성화되어야 합니다 | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| GuardDuty.10 | GuardDuty S3 보호를 활성화해야 합니다 | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| GuardDuty.11 | GuardDuty 런타임 모니터링을 활성화해야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 주기적 |
| GuardDuty.12 | GuardDuty ECS 런타임 모니터링을 활성화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| GuardDuty.13 | GuardDuty EC2 런타임 모니터링을 활성화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.1 | IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, CIS AWS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| IAM.2 | IAM 사용자는 IAM 정책을 연결해서는 안 됩니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.3 | IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.4 | IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 심각 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.5 | 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.6 | 루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 주기적 |
| IAM.7 | IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊙ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.8 | 사용하지 않은 IAM 사용자 보안 인증은 제거해야 합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v3.2.1, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.9 | 루트 사용자에 대해 MFA를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 주기적 |
| IAM.10 | IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다. | NIST SP 800-171 개정 2, PCI DSS v3.2.1 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.11 | IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.12 | IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.13 | IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.14 | IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.15 | IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.16 | IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 주기적 |
| IAM.17 | IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다. | CIS AWS 파운데이션 벤치마크 v1.2.0, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 주기적 |
| IAM.18 | AWS Support 를 통해 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 주기적 |
| IAM.19 | 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다. | NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v3.2.1, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.21 | 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| IAM.22 | 45일 동안 사용하지 않은 IAM 사용자 보안 인증은 제거해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.23 | IAM Access Analyzer 분석기에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IAM.24 | IAM 역할에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IAM.25 | IAM 사용자에게 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IAM.26 | IAM에서 관리되는 만료된 SSL/TLS 인증서는 제거해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0 | 중간 | ⊗ 아니요 | 주기적 |
| IAM.27 | IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IAM.28 | IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0 | 높음 | ⊗ 아니요 | 주기적 |
| Inspector.1 | Amazon Inspector EC2 스캔을 활성화해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| Inspector.2 | Amazon Inspector ECR 스캔을 활성화해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| Inspector.3 | Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| Inspector.4 | Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| IoT.1 | AWS IoT Device Defender 보안 프로필에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoT.2 | AWS IoT Core 완화 작업에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoT.3 | AWS IoT Core 차원에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IoT.4 | AWS IoT Core 권한 부여자에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoT.5 | AWS IoT Core 역할 별칭에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoT.6 | AWS IoT Core 정책에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoTSiteWise.1 | AWS IoT SiteWise 자산 모델에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoTSiteWise.2 | AWS IoT SiteWise 대시보드에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoTSiteWise.3 | AWS IoT SiteWise 게이트웨이에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoTSiteWise.4 | AWS IoT SiteWise 포털에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| IoTSiteWise.5 | AWS IoT SiteWise 프로젝트에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IoTTwinMaker.1 | AWS IoT TwinMaker 동기화 작업에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IoTTwinMaker.2 | AWS IoT TwinMaker 워크스페이스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IoTTwinMaker.3 | AWS IoT TwinMaker 장면에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IoTTwinMaker.4 | AWS IoT TwinMaker 엔터티에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IoTWireless.1 | AWS IoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IoTWireless.2 | AWS IoT Wireless 서비스 프로파일에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IoTWireless.3 | AWS IoT Wireless FUOTA 작업에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IVS.1 | IVS 재생 키 페어에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| IVS.2 | IVS 레코딩 구성에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| IVS.3 | IVS 채널에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Keyspaces.1 | Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Kinesis.1 | Kinesis 스트림은 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| Kinesis.2 | Kinesis 스트림에는 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Kinesis.3 | Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✓ 예 | 변경이 트리거됨 |
| KMS.1 | IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| KMS.2 | IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| KMS.3 | AWS KMS keys 실수로 삭제해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 심각 | ✗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| KMS.4 | AWS KMS key 교체를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, CIS AWS 파운데이션 벤치마크 v1.2.0, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| KMS.5 | KMS 키는 공개적으로 액세스할 수 없어야 합니다. | AWS 기본 보안 모범 사례 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| Lambda.1 | Lambda 함수는 퍼블릭 액세스를 금지해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| Lambda.2 | Lambda 함수는 최신 런타임을 사용해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Lambda.3 | Lambda 함수는 VPC에 있어야 합니다. | PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| Lambda.5 | VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Lambda.6 | Lambda 함수는 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Lambda.7 | Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다. | NIST SP 800-53 개정 5 | 낮음 | ✗ 아니요 | 변경이 트리거됨 |
| Macie.1 | Amazon Macie가 활성화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 주기적 |
| Macie.2 | Macie의 민감한 데이터 자동 검색을 활성화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ✗ 아니요 | 주기적 |
| MSK.1 | MSK 클러스터는 브로커 노드 간에 전송되는 동안 암호화되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| MSK.2 | MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다. | NIST SP 800-53 개정 5 | 낮음 | ✗ 아니요 | 변경이 트리거됨 |
| MSK.3 | MSK Connect 커넥터는 전송 중에 암호화해야 합니다 | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| MSK.4 | MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 심각 | ✗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| MSK.5 | MSK 커넥터에는 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| MSK.6 | MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| MQ.2 | ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| MQ.4 | Amazon MQ 브로커에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| MQ.5 | ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다. | NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| MQ.6 | RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다. | NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| Neptune.1 | Neptune DB 클러스터는 저장 시 암호화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Neptune.2 | Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Neptune.3 | Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| Neptune.4 | Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| Neptune.5 | Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 변경이 트리거됨 |
| Neptune.6 | Neptune DB 클러스터 스냅샷은 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Neptune.7 | Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Neptune.8 | 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| Neptune.9 | Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다. | NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| NetworkFirewall.1 | Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다. | NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| NetworkFirewall.2 | Network Firewall 로깅을 활성화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 주기적 |
| NetworkFirewall.3 | Network Firewall 정책에는 적어도 하나의 규칙 그룹이 연결되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| NetworkFirewall.4 | 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| NetworkFirewall.5 | 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| NetworkFirewall.6 | 상태 비저장 네트워크 방화벽 규칙 그룹은 비워둘 수 없습니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| NetworkFirewall.7 | Network Firewall 방화벽에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| NetworkFirewall.8 | Network Firewall 방화벽 정책에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| NetworkFirewall.9 | Network Firewall 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| NetworkFirewall.10 | Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| Opensearch.1 | OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| Opensearch.2 | OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 심각 | ✗ 아니요 | 변경이 트리거됨 |
| Opensearch.3 | OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Opensearch.4 | CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅을 활성화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Opensearch.5 | OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Opensearch.6 | OpenSearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Opensearch.7 | OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| Opensearch.8 | OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Opensearch.9 | OpenSearch 도메인에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| Opensearch.10 | OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Opensearch.11 | OpenSearch 도메인에는 최소 세 개의 전용 프라이머리 노드가 있어야 합니다. | NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 주기적 |
| PCA.1 | AWS Private CA 루트 인증 기관은 비활성화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 주기적 |
| PCA.2 | AWS 프라이빗 CA 인증 기관에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| RDS.1 | RDS 스냅샷은 비공개 상태여야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.2 | RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.3 | RDS DB 인스턴스에서 저장 시 암호화를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.4 | RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.5 | RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.6 | RDS DB 인스턴스에 대해 향상된 모니터링을 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| RDS.7 | RDS 클러스터에는 삭제 보호 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.8 | RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.9 | RDS DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.10 | RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.11 | RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊘ 예 | 변경이 트리거됨 |
| RDS.12 | RDS 클러스터에 대해 IAM 인증을 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.13 | RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.14 | Amazon Aurora 클러스터에는 백트래킹이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊘ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.15 | RDS DB 클러스터는 여러 가용 영역에 맞게 구성해야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.16 | 태그를 DB 스냅샷에 복사하도록 Aurora DB 클러스터를 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.17 | 태그를 스냅샷에 복사하도록 RDS DB 인스턴스를 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.19 | 기존 RDS 이벤트 알림 구독은 중요 클러스터 이벤트에 맞게 구성해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.20 | 기존 RDS 이벤트 알림 구독은 중요한 데이터베이스 인스턴스 이벤트에 맞게 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.21 | 중요한 데이터베이스 파라미터 그룹 이벤트에 대해서는 RDS 이벤트 알림 구독을 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.22 | 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.23 | RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.24 | RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.25 | RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.26 | RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다. | NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 주기적 |
| RDS.27 | RDS DB 클러스터는 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.28 | RDS DB 클러스터에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.29 | RDS DB 클러스터 스냅샷에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| RDS.30 | RDS DB 인스턴스에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| RDS.31 | RDS DB 보안 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| RDS.32 | RDS DB 스냅샷에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| RDS.33 | RDS DB 서브넷 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| RDS.34 | Aurora MySQL DB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| RDS.35 | RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| RDS.36 | RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 중간 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.37 | Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.38 | RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| RDS.39 | RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| RDS.40 | RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 변경이 트리거됨 |
| RDS.41 | RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| RDS.42 | RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ✓ 예 | 주기적 |
| RDS.43 | RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.44 | RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| RDS.45 | Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| RDS.46 | RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 주기적 |
| RDS.47 | 태그를 DB 스냅샷에 복사하도록 RDS for PostgreSQL DB 클러스터를 구성해야 합니다. | AWS 기본 보안 모범 사례 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.48 | 태그를 DB 스냅샷에 복사하도록 RDS for MySQL DB 클러스터를 구성해야 합니다. | AWS 기본 보안 모범 사례 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| RDS.50 | RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RDS.51 | RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.1 | Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.2 | Amazon Redshift 클러스터에 대한 연결은 전송 중에 암호화되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.3 | Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 변경이 트리거됨 |
| Redshift.4 | Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.6 | Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Redshift.7 | Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.8 | Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.10 | Redshift 클러스터는 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.11 | Redshift 클러스터에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Redshift.12 | Redshift 이벤트 구독 알림에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Redshift.13 | Redshift 클러스터 스냅샷에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Redshift.14 | Redshift 클러스터 서브넷 그룹에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Redshift.15 | Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다. | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Redshift.16 | Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다. | NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Redshift.17 | Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Redshift.18 | Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| RedshiftServerless.1 | Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 주기적 |
| RedshiftServerless.2 | Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| RedshiftServerless.3 | Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 주기적 |
| RedshiftServerless.4 | Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다. AWS KMS keys | NIST SP 800-53 개정 5 | 중간 | ⊙ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| RedshiftServerless.5 | Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| RedshiftServerless.6 | Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| Route53.1 | Route 53 상태 확인에는 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Route53.2 | Route 53 퍼블릭 호스팅 영역은 DNS 쿼리를 기록해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.1 | S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| S3.2 | S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다 | AWS 기본 보안 모범 사례, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 심각 | ⊗ 아니요 | 변경이 트리거되고 주기적입니다. |
| S3.3 | S3 범용 버킷은 퍼블릭 쓰기 액세스를 차단해야 합니다 | AWS 기본 보안 모범 사례, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 심각 | ⊗ 아니요 | 변경이 트리거되고 주기적입니다. |
| S3.5 | S3 범용 버킷은 SSL 사용 요청이 필요합니다 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v3.2.1, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.6 | S3 범용 버킷 정책은 다른에 대한 액세스를 제한해야 합니다. AWS 계정 | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.7 | S3 범용 버킷은 리전 간 복제를 사용해야 합니다 | PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| S3.8 | S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.9 | S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다 | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.10 | 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다 | NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.11 | S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다 | NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊘ 예 | 변경이 트리거됨 |
| S3.12 | S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다 | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.13 | S3 범용 버킷에는 수명 주기 구성이 있어야 합니다 | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 낮음 | ⊘ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| S3.14 | S3 범용 버킷에는 버전 관리가 활성화되어 있어야 합니다 | NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.15 | S3 범용 버킷에는 Object Lock이 활성화되어 있어야 합니다 | NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊙ 예 | 변경이 트리거됨 |
| S3.17 | S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys | NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.19 | S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.20 | S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다. | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, CIS AWS 파운데이션 벤치마크 v1.4.0, NIST SP 800-53 개정 5 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.22 | S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| S3.23 | S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다 | CIS AWS 파운데이션 벤치마크 v5.0.0, CIS AWS 파운데이션 벤치마크 v3.0.0, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| S3.24 | S3 다중 리전 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다 | AWS 기본 보안 모범 사례, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| S3.25 | S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다 | AWS 기본 보안 모범 사례 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| SageMaker.1 | Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 주기적 |
| SageMaker.2 | SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.3 | 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| SageMaker.4 | SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 주기적 |
| SageMaker.5 | SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.6 | SageMaker 앱 이미지 구성에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| SageMaker.7 | SageMaker 이미지에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| SageMaker.8 | SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 주기적 |
| SageMaker.9 | SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.10 | SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| SageMaker.11 | SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.12 | SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.13 | SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.14 | SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.15 | SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.16 | SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| SageMaker.17 | SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.18 | 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다. | NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.19 | SageMaker 모델은 멀티컨테이너 추론 파이프라인에 VPC의 프라이빗 레지스트리를 사용해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.20 | SageMaker 모델 설명 가능성 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.21 | SageMaker 노트북 인스턴스는 고객 관리형 AWS KMS 키로 암호화해야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.22 | SageMaker 모니터링 일정에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| SageMaker.23 | SageMaker 추론 실험에는 고객 관리형 AWS KMS 키로 암호화된 인스턴스 스토리지 볼륨이 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.24 | SageMaker 추론 실험에는 고객 관리형 AWS KMS 키로 암호화된 데이터 스토리지가 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SageMaker.25 | SageMaker 모델 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| SecretsManager.1 | Secrets Manager 비밀 번호에는 자동 로테이션이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊘ 예 | 변경이 트리거됨 |
| SecretsManager.2 | 자동 교체로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SecretsManager.3 | 사용하지 않는 Secrets Manager 암호를 제거합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊘ 예 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| SecretsManager.4 | Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ✓ 예 | 주기적 |
| SecretsManager.5 | Secrets Manager 보안 암호에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| ServiceCatalog.1 | Service Catalog 포트폴리오는 AWS 조직 내에서만 공유해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ✗ 아니요 | 주기적 |
| SES.1 | SES 연락처 목록에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| SES.2 | SES 구성 세트에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| SES.3 | SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| SNS.1 | SNS 주제는를 사용하여 유휴 시 암호화되어야 합니다. AWS KMS | NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ✗ 아니요 | 변경이 트리거됨 |
| SNS.3 | SNS 주제에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| SNS.4 | SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다. | AWS 기본 보안 모범 사례 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| SQS.1 | Amazon SQS 대기열은 저장 시 암호화해야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SQS.2 | SQS 대기열에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ✓ 예 | 변경이 트리거됨 |
| SQS.3 | SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다. | AWS 기본 보안 모범 사례 | 심각 | ⊗ 아니요 | 변경이 트리거됨 |
| SSM.1 | EC2 인스턴스는에서 관리해야 합니다. AWS Systems Manager | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v3.2.1, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| SSM.2 | Systems Manager가 관리하는 EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2, PCI DSS v3.2.1, PCI DSS v4.0.1 | 높음 | ⊗ 아니요 | 변경이 트리거됨 |
| SSM.3 | Systems Manager에서 관리하는 EC2 인스턴스의 연결 규정 준수 상태는 COMPLIANT여야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, PCI DSS v3.2.1, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| SSM.4 | SSM 문서는 공개해서는 안 됩니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 심각 | ⊗ 아니요 | 주기적 |
| SSM.5 | SSM 문서에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| SSM.6 | SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 중간 | ⊗ 아니요 | 주기적 |
| SSM.7 | SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0 | 심각 | ⊗ 아니요 | 주기적 |
| StepFunctions.1 | Step Functions 상태 머신은 로깅이 켜져 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, PCI DSS v4.0.1 | 중간 | ⊙ 예 | 변경이 트리거됨 |
| StepFunctions.2 | Step Functions 작업에는 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Transfer.1 | Transfer Family 워크플로에 태그를 지정해야 합니다. | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Transfer.2 | Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다 | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| Transfer.3 | Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| Transfer.4 | Transfer Family 계약에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Transfer.5 | Transfer Family 인증서에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Transfer.6 | Transfer Family 커넥터에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| Transfer.7 | Transfer Family 프로파일에 태그를 지정해야 합니다 | AWS 리소스 태그 지정 표준 | 낮음 | ⊙ 예 | 변경이 트리거됨 |
| WAF.1 | AWS WAF Classic Global Web ACL 로깅을 활성화해야 합니다. | AWS 기본 보안 모범 사례, NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 중간 | ⊗ 아니요 | 주기적 |
| WAF.2 | AWS WAF Classic 리전 규칙에는 하나 이상의 조건이 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| WAF.3 | AWS WAF Classic 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WAF.4 | AWS WAF Classic 리전 웹 ACLs 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WAF.6 | AWS WAF Classic 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WAF.7 | AWS WAF Classic 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WAF.8 | AWS WAF Classic 글로벌 웹 ACLs 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WAF.10 | AWS WAF 웹 ACLs 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WAF.11 | AWS WAF 웹 ACL 로깅을 활성화해야 합니다. | NIST SP 800-53 개정 5, PCI DSS v4.0.1 | 낮음 | ⊗ 아니요 | 주기적 |

| 보안 제어 ID | 보안 제어 제목 | 적용 가능한 표준 | 심각도 | 사용자 지정 파라미터를 지원합니다. | 일정 유형 |
|---|---|---|---|---|---|
| WAF.12 | AWS WAF 규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다. | AWS 기본 보안 모범 사례 v1.0.0, NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WorkSpaces.1 | WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다 | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |
| WorkSpaces.2 | WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다 | AWS 기본 보안 모범 사례 | 중간 | ⊗ 아니요 | 변경이 트리거됨 |

## Security Hub CSPM 제어의 변경 로그

다음 변경 로그는 기존 AWS Security Hub CSPM 제어에 대한 중요한 변경 사항을 추적하여 제어의 전체 상태와 조사 결과의 규정 준수 상태가 변경될 수 있습니다. Security Hub CSPM이 제어의 상태를 평가하는 방법에 대한 자세한 내용은 규정 준수 상태 및 제어 상태 평가 섹션을 참조하세요. 변경 사항이 이 로그에 입력된 후 컨트롤을 사용할 수 있는 모든 AWS 리전 에 영향을 미치는 데 며칠이 걸릴 수 있습니다.

이 로그는 2023년 4월 이후 발생한 변경 사항을 추적합니다. 제어를 선택하여 해당 제어에 대한 추가 세부 정보를 검토합니다. 제목 변경 사항은 90일 동안 해당 제어의 세부 설명에 기록됩니다.

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
|---|---|---|
| 2026년 9월 11일 | [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다. | 이 제어는 Amazon RDS DB 클러스터에 대해 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. Security Hub |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| | | CSPM은 이전에 조사 결과를 반환하지 않았던 Aurora DB 클러스터를 평가하도록 제어를 확장했습니다. |
| 2026년 9월 11일 | [S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다. | Security Hub CSPM은 SSL이 더 이상 사용되지 않으므로 SSL 대신 TLS를 참조하도록이 컨트롤의 제목과 설명을 업데이트했습니다. |
| 2026년 8월 27일 | [RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다. | 이 제어는 Amazon RDS 인스턴스가 퍼블릭 액세스를 금지하는지 여부를 확인합니다. Neptune DB는 이제 퍼블릭 엔드포인트를 지원하므로이 제어는 Neptune DB 인스턴스에 대해 실행 가능한 결과를 평가하고 생성합니다. Security Hub CSPM은이 변경 사항을 반영하도록 제어 설명을 업데이트했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 8월 12일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon EKS 클러스터가 지원되는 Kubernetes 버전에서 실행되는지 여부를 확인합니다. Security Hub CSPM은 이 제어의 파라미터 값을 `1.33`에서 `1.34`로 변경했습니다. Amazon EKS의 Kubernetes 버전 1.33에 대한 표준 지원은 2026년 7월 29일에 종료되었습니다. |
| 2026년 8월 12일 | [EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon EKS 노드 그룹이 지원되는 Kubernetes 버전에서 실행되는지 확인합니다. Security Hub CSPM은 이 제어의 파라미터 값을 `1.33`에서 `1.34`로 변경했습니다. Amazon EKS의 Kubernetes 버전 1.33에 대한 표준 지원은 2026년 7월 29일에 종료되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 8월 3일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 AWS Lambda 가이 런타임에 대한 지원을 추가했으므로를 `java17.al2023, java11.al2023, java8.al2023` 파라미터 값으로 지원합니다. |
| 2026년 8월 3일 | [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에서 이 제어를 제거했습니다. |
| 2026년 7월 31일 | [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다 | Security Hub CSPM은 이 제어의 파라미터 값을 `notebook-al2-v3`에서 `notebook-al2023-v1` 로 변경했습니다. SageMaker AI는 노트북 인스턴스 플랫폼을 Amazon Linux 2에서 AL2023으로 마이그레이션했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 7월 13일 | [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다. | Security Hub CSPM 은이 제어에 대한 지원 규칙을 service-vpc-endpoint-enabled에서 vpc-endpoint-enabled로 변경했습니다. 업데이트된 규칙은 FIPS 변형 엔드포인트 서비스 이름을 규정 준수로 인식하고 FIPS 엔드포인트를 사용하는 VPCs에 대한 PASSED 결과를 생성합니다. |
| 2026년 6월 29일 | [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다 | Security Hub CSPM 은 NIST SP 800-53 개정 5 표준, NIST SP 800-171 개정 2 표준 및 PCI DSS v4.0.1 표준과 같은 적용 가능한 표준에이 제어를 추가했습니다. 2026년 7월 30일에이 제어는 AWS 기본 보안 모범 사례 (FSBP) 표준에서 제거됩니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 6월 5일 | [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다. | Security Hub CSPM은 2026년 8월 10일 이후이 제어가 사용 중지되고 모든 해당 Security Hub CSPM 표준에서 제거된다는 알림을 제공했습니다. Kubernetes 버전 1.28부터 Amazon EKS 클러스터에는 기본적으로 봉투 암호화로 보호되는 Kubernetes 보안 암호가 있습니다. |
| 2026년 6월 5일 | [IoTEvents.1] IoTEvents.1 | Security Hub CSPM은 2026년 7월 7일 이후이 제어가 사용 중지되고 모든 해당 Security Hub CSPM 표준에서 제거된다는 알림을 제공했습니다. AWS 는 2026년 5월 20일부터 AWS IoT Events 서비스에 대한 지원 종료를 발표했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 6월 5일 | [IoTEvents.2] IoTEvents.2 | Security Hub CSPM은 2026년 7월 7일 이후 이 제어가 사용 중지되고 모든 해당 Security Hub CSPM 표준에서 제거된다는 알림을 제공했습니다. AWS 는 2026년 5월 20일부터 AWS IoT Events 서비스에 대한 지원 종료를 발표했습니다. |
| 2026년 6월 5일 | [IoTEvents.3] IoTEvents.3 | Security Hub CSPM은 2026년 7월 7일 이후 이 제어가 사용 중지되고 모든 해당 Security Hub CSPM 표준에서 제거된다는 알림을 제공했습니다. AWS 는 2026년 5월 20일부터 AWS IoT Events 서비스에 대한 지원 종료를 발표했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 6월 5일 | [ECS.1] Amazon ECS 태스크 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다 | Security Hub CSPM 은이 제어를 사용 중지하고 적용 가능한 모든 표준에서 제거했습니다. 이전에는 제어에서 호스트 네트워킹 모드를 사용한 활성 Amazon ECS 태스크 정의에 `privileged` 또는 `user` 컨테이너 정의도 있는지 확인했습니다. |
| 2026년 6월 5일 | [RDS.18] RDS 인스턴스는 VPC에 배포되어야 합니다. | Security Hub CSPM 은이 제어를 사용 중지하고 적용 가능한 모든 표준에서 제거했습니다. Amazon EC2-Classic 네트워킹이 사용 중지되었으므로 Amazon Relational Database Service(Amazon RDS) 인스턴스는 더 이상 VPC 외부에 배포할 수 없습니다. 이전에는 제어가 Amazon RDS 인스턴스가 EC2-VPC에 배포되었는지 여부를 확인했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 5월 4일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제를 파라미터ruby4.0로 지원하며 AWS Lambda 가이 런타임을 더 이상 사용하지 nodejs20.x 않으므로를 더 이상 포함하지 않습니다. |
| 2026년 4월 27일 | [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다. | Security Hub CSPM은이 제어에 대한 지원 규칙을 ec2-stopped-instance에서 사용자 지정 Security Hub CSPM 규칙인 ec2-stopped-instance-days-check로 변경하여 평가 로직을 간소화했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 4월 7일 | [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원 가능하도록 구성해서는 안 됩니다. | Security Hub CSPM은 이 제어의 제목 및 설명을 변경했습니다. 새로운 제목과 설명은 제어가 Amazon EBS 스냅샷이 공개적으로 복원 가능하도록 구성되어 있는지 여부를 확인하는 것을 보다 정확하게 반영합니다. 이전에는이 제어의 제목이 다음과 같았습니다. Amazon EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다. |
| 2026년 4월 7일 | [EC2.182] Amazon EBS 스냅샷에 대해 퍼블릭 액세스 차단 설정을 활성화해야 합니다. | Security Hub CSPM은 이 제어의 제목 및 설명을 변경했습니다. 새로운 제목과 설명은 제어가 Amazon EBS 스냅샷에 대해 계정 수준 퍼블릭 액세스 차단이 활성화되어 있는지 여부를 확인하는 것을 보다 정확하게 반영합니다. 이전에는이 제어의 제목이 다음과 같았습니다. Amazon EBS 스냅샷에 공개적으로 액세스할 수 없어야 합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 4월 6일 | [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다 | Security Hub CSPM은 권장 보안 정책을 반영하도록이 제어의 파라미터 값을 업데이트했습니다. |
| 2026년 4월 3일 | [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다 | Security Hub CSPM은 이 제어의 `temporaryPasswordValidity` 파라미터에 대해 지원되는 값의 범위를 확장했습니다. 이제 1~365일 범위의 값을 지정할 수 있습니다. 이전에는 범위가 7~365일이었습니다. |
| 2026년 4월 3일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon EKS 클러스터가 지원되는 Kubernetes 버전에서 실행되는지 여부를 확인합니다. Security Hub CSPM은 이 제어의 파라미터 값을 `1.32`에서 `1.33`로 변경했습니다. Amazon EKS의 Kubernetes 버전 1.32에 대한 표준 지원은 2026년 3월 23일에 종료되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 4월 3일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda는이 런타임을 더 이상 사용하지 `ruby3.2` 않으므로 지원되는 런타임에 대한 Lambda.2 파라미터에는가 더 이상 포함되지 않습니다. |
| 2026년 3월 24일 | [RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다. | Security Hub CSPM은 제어가 모든 RDS DB 클러스터를 검사함을 반영하도록 제어 제목을 업데이트했습니다. |
| 2026년 3월 24일 | [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다. | Security Hub CSPM은 제어가 ECS 작업 정의를 확인하는 것을 반영하도록 제어 제목과 설명을 업데이트했습니다. Security Hub CSPM은 `WINDOWS_SERVER` OS 패밀리를 지정하도록 `runtimePlatform` 구성된를 사용하여 작업 정의에 대한 결과를 생성하지 않도록 컨트롤도 업데이트했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 3월 9일 | [AppSync.1] AWS AppSync API 캐시는 저장 시 암호화되어야 합니다. | Security Hub CSPM 은이 제어를 사용 중지하고 AWS 기본 보안 모범 사례(FSBP) 표준에서 제거했습니다. 는 AWS AppSync 이제 모든 현재 및 향후 API 캐시에 대한 기본 암호화를 제공합니다. |
| 2026년 3월 9일 | [AppSync.6] AWS AppSync API 캐시는 전송 중에 암호화되어야 합니다. | Security Hub CSPM 은이 제어를 사용 중지하고 AWS 기본 보안 모범 사례(FSBP) 표준에서 제거했습니다. 는 AWS AppSync 이제 모든 현재 및 향후 API 캐시에 대한 기본 암호화를 제공합니다. |
| 2026년 3월 4일 | [ECS.1] Amazon ECS 태스크 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다 | Security Hub CSPM 은이 제어를 사용 중지하고 AWS FSBP(기본 보안 모범 사례) 표준 및 NIST SP 800-53 개정 5 표준에서 제거했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 2월 5일 | [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다. | Security Hub CSPM은 2026년 3월 9일에 이 제어를 사용 중지하고 해당하는 모든 Security Hub CSPM 표준에서 제거합니다. AWS AppSync 는 모든 현재 및 향후 API 캐시에 기본 암호화를 제공합니다. |
| 2026년 2월 5일 | [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다. | Security Hub CSPM은 2026년 3월 9일에 이 제어를 사용 중지하고 해당하는 모든 Security Hub CSPM 표준에서 제거합니다. AWS AppSync 는 모든 현재 및 향후 API 캐시에 기본 암호화를 제공합니다. |
| 2026년 1월 16일 | [ECS.1] Amazon ECS 태스크 정의에는 보안 네트워킹 모드와 사용자 정의가 있어야 합니다 | Security Hub CSPM은 2026년 2월 16일 이후 이 제어가 사용 중지되고 모든 해당 Security Hub CSPM 표준에서 제거된다는 알림을 제공했습니다. |
| 2026년 1월 12일 | [Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. | Security Hub CSPM은 `loggingEnabled` 파라미터를 제거하도록이 제어를 업데이트했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2026년 1월 12일 | [MQ.3] Amazon MQ 브로커에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다. | Security Hub CSPM은 제어를 사용 중지하고 적용 가능한 모든 표준에서 제어를 제거했습니다. Security Hub CSPM은 자동 마이너 버전 업그레이드에 대한 Amazon MQ 요구 사항으로 인해 제어를 사용 중지했습니다.<br><br>이전에는 AWS FSBP(기본 보안 모범 사례) 표준, NIST SP 800-53 개정 5 표준 및 PCI DSS v4.0.1 표준에 제어가 적용되었습니다. |
| 2026년 1월 12일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | 이 제어는 AWS Lambda 함수의 런타임 설정이 각 언어에서 지원되는 런타임의 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제이 컨트롤에 대한 파라미터 값으로 `dotnet10`를 지원합니다.이 런타임에 대한 지원이 AWS Lambda 추가되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 12월 15일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | 이 제어는 AWS Lambda 함수의 런타임 설정이 각 언어에서 지원되는 런타임의 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 더 이상 이 컨트롤의 파라미터 값으로 `python3.9` 를 지원하지 않습니다.는 더 이상이 런타임을 지원하지 AWS Lambda 않습니다. |
| 2025년 12월 12일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon EKS 클러스터가 지원되는 Kubernetes 버전에서 실행되는지 여부를 확인합니다. Security Hub CSPM은 이 제어의 파라미터 값을 `1.31`에서 `1.32`로 변경했습니다. Amazon EKS의 Kubernetes 버전 1.31에 대한 표준 지원은 2025년 11월 26일에 종료되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 11월 21일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | 이 제어는 AWS Lambda 함수의 런타임 설정이 각 언어에서 지원되는 런타임의 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제이 컨트롤에 대한 `python3.14` 파라미터 값으로 `nodejs24.x` 및를 지원합니다. 이러한 런타임에 대한 지원이 AWS Lambda 추가되었습니다. |
| 2025년 11월 14일 | [EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다. | Security Hub CSPM은이 제어에 대한 설명과 근거를 업데이트했습니다. 이전에는 플래그를 사용하여 Amazon VPC 서브넷에서 IPv4 퍼블릭 IP 자동 할당만 확인했습니다`MapPublicIpOnLaunch`. 이제이 제어는 IPv4 및 IPv6 퍼블릭 IP 자동 할당을 모두 확인합니다. 이러한 변경 사항을 반영하도록 컨트롤의 설명 및 근거가 업데이트되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 11월 14일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | 이 제어는 AWS Lambda 함수의 런타임 설정이 각 언어에서 지원되는 런타임의 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 이 제어의 파라미터 값으로 `java25`를 지원합니다. AWS Lambda는 이 런타임에 대한 지원을 추가했습니다. |
| 2025년 11월 13일 | [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다. | Security Hub CSPM은 이 제어의 심각도를 `HIGH`에서 `CRITICAL`로 변경했습니다. Amazon SNS 주제에 대한 퍼블릭 액세스를 허용하면 상당한 보안 위험이 있습니다. |
| 2025년 11월 13일 | [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다 | Security Hub CSPM은 이 제어의 심각도를 `HIGH`에서 `CRITICAL`로 변경했습니다. Amazon SQS 대기열에 대한 퍼블릭 액세스를 허용하면 상당한 보안 위험이 발생합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 11월 13일 | [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다. | Security Hub CSPM은 이 제어의 심각도를 에서 MEDIUM로 변경했습니다HIGH. 이러한 유형의 런타임 모니터링은 Amazon EKS 리소스에 대한 향상된 위협 탐지를 제공합니다. |
| 2025년 11월 13일 | [MQ.3] Amazon MQ 브로커에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다. | Security Hub CSPM은 이 제어의 심각도를 에서 LOW로 변경했습니다MEDIUM. 마이너 버전 업그레이드에는 Amazon MQ 브로커 보안을 유지하는 데 필요한 보안 패치가 포함됩니다. |
| 2025년 11월 13일 | [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다. | Security Hub CSPM은 이 제어의 심각도를에서 LOW로 변경했습니다MEDIUM. 소프트웨어 업데이트에는 OpenSearch 도메인 보안을 유지하는 데 필요한 보안 패치가 포함됩니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 11월 13일 | [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다. | Security Hub CSPM은 이 제어의 심각도를 에서 LOW로 변경했습니다MEDIUM. 삭제 방지 기능은 Amazon RDS 데이터베이스가 실수로 삭제되고 권한이 없는 엔터티가 RDS 데이터베이스를 삭제하는 것을 방지하는 데 도움이 됩니다. |
| 2025년 11월 13일 | [CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. | Security Hub CSPM은 이 제어의 심각도를 에서 LOW로 변경했습니다MEDIUM. Amazon CloudWatch Logs의 AWS CloudTrail 로깅 데이터는 감사 활동, 경보 및 기타 중요한 보안 작업에 사용할 수 있습니다. |
| 2025년 11월 13일 | [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다. | Security Hub CSPM은 이 제어의 심각도를 에서 HIGH로 변경했습니다MEDIUM. AWS Service Catalog 포트폴리오를 특정 계정과 공유하는 것은 의도적인 것일 수 있으며 포트폴리오에 공개적으로 액세스할 수 있음을 반드시 나타내는 것은 아닙니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 11월 13일 | [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다. | Security Hub CSPM은 이 제어의 심각도를에서 MEDIUM로 변경했습니다LOW. Amazon CloudFront 배포의 기본 cloudfront.net 도메인 이름은 무작위로 생성되므로 보안 위험이 줄어듭니다. |
| 2025년 11월 13일 | [ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다. | Security Hub CSPM은이 제어의 심각도를에서 MEDIUM로 변경했습니다LOW. 다중 인스턴스 배포에서 다른 정상 인스턴스는 연결 드레이닝 없이 인스턴스가 종료될 때 사용자 세션을 처리할 수 있으므로 운영 영향과 가용성 위험이 줄어듭니다. |
| 2025년 11월 13일 | [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다 | Security Hub CSPM은 선택적 validAdminUserNames 파라미터를 제거하도록이 제어를 업데이트했습니다. |
| 2025년 10월 23일 | [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다. | Security Hub CSPM은 2025년 10월 14일에 이 제어의 제목, 설명 및 규칙에 적용된 변경 사항을 되돌렸습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 10월 22일 | [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다. | Security Hub CSPM은 사용자 지정 오리진을 사용하는 Amazon CloudFront 배포에 대한 조사 결과를 생성하지 않도록 이 제어를 업데이트했습니다. |
| 2025년 10월 16일 | [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다 | 이 제어는 Amazon CloudFront 배포가 권장 TLS 보안 정책을 사용하도록 구성되어 있는지 확인합니다. Security Hub CSPM은 이제 이 제어의 파라미터 값으로 `TLSv1.2_2025` 및 `TLSv1.3_2025` 를 지원합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 10월 14일 | [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다. | Security Hub CSPM이 이 제어의 제목, 설명 및 규칙을 변경했습니다. 이전에는 이 제어가 elasticache-redis-cluster-automatic-backup-check 규칙을 사용하여 Redis OSS 클러스터 및 모든 복제 그룹을 확인했습니다. 이 제어의 제목은 ElastiCache(Redis OSS) 클러스터에 자동 백업이 활성화되어 있어야 합니다였습니다.<br><br>이제 이 제어는 elasticache-automatic-backup-check-enabled 규칙을 사용하여 Redis OSS 클러스터 및 모든 복제 그룹 외에도 Valkey 클러스터를 확인합니다. 새 제목 및 설명은 이 제어가 두 유형의 클러스터를 모두 확인함을 반영합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 10월 5일 | [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다. | Amazon OpenSearch Service 도메인에 사용 가능한 소프트웨어 업데이트가 없고 업데이트 상태가 부적격인 경우에도 PASSED 조사 결과를 생성하도록 이 제어에 대한 규칙이 업데이트되었습니다. 이전에는 이 제어가 OpenSearch 도메인에 사용 가능한 소프트웨어 업데이트가 없고 업데이트 상태가 완료인 경우에만 PASSED 조사 결과를 생성했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 9월 24일 | [Redshift.9] Redshift 클러스터는 기본 데이터베이스 이름을 사용해서는 안 됩니다.<br><br>[RedshiftServerless.7] Redshift Serverless 네임스페이스는 기본 데이터베이스 이름을 사용해서는 안 됩니다 | Security Hub CSPM은 이들 제어를 사용 중지했고 모든 관련 표준에서 제거했습니다. Security Hub CSPM은 이러한 제어에 대한 `FAILED` 조사 결과를 효과적으로 수정할 수 없었던 Amazon Redshift에 내재된 제한으로 인해 제어를 사용 중지했습니다.<br><br>이전에는 이러한 제어가 AWS 기본 보안 모범 사례(FSBP) 표준 및 NIST SP 800-53 개정 5 표준에 적용되었습니다. Redshift.9 제어는 AWS Control Tower 서비스 관리형 표준에도 적용되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 9월 9일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | 이 제어는 AWS Lambda 함수의 런타임 설정이 각 언어에서 지원되는 런타임의 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 더 이상 이 제어의 파라미터 값으로 `nodejs18.x` 를 지원하지 않습니다. AWS Lambda 는 더 이상 Node.js 18 런타임을 지원하지 않습니다. |
| 2025년 8월 13일 | [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다 | Security Hub CSPM은 이 제어의 제목 및 설명을 변경했습니다. 새로운 제목 및 설명은 제어가 Amazon SageMaker AI 호스팅 모델의 `EnableNetworkIsolation` 파라미터에 대한 설정을 확인함을 보다 정확하게 반영합니다. 이전에는 이 제어의 제목이 SageMaker models should block inbound traffic였습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 8월 13일 | [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다 | Security Hub CSPM은 이 제어의 제목 및 설명을 변경했습니다. 새로운 제목 및 설명은 제어가 수행하는 검사의 범위와 특성을 더 정확하게 반영합니다. 이전에는 이 제어의 제목이 EFS mount targets should not be associated with a public subnet였습니다. |
| 2025년 7월 24일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon EKS 클러스터가 지원되는 Kubernetes 버전에서 실행되는지 여부를 확인합니다. Security Hub CSPM은 이 제어의 파라미터 값을 `1.30`에서 `1.31`로 변경했습니다. Amazon EKS의 Kubernetes 버전 1.30에 대한 표준 지원은 2025년 7월 23일에 종료되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 7월 23일 | [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다 | Security Hub CSPM은 이 제어의 제목을 변경했습니다. 새로운 제목은 제어가 시작 파라미터를 지정하는 Amazon EC2 스팟 플릿 요청만 확인함을 더 정확하게 반영합니다. 이전에는 이 제어의 제목이 EC2 Spot Fleet requests should enable encryption for attached EBS volumes였습니다. |
| 2025년 6월 30일 | [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다. | Security Hub CSPM은 PCI DSS v4.0.1 표준에서 이 제어를 제거했습니다. PCI DSS v4.0.1은 암호에 기호를 사용하도록 명시적으로 요구하지 않습니다. |
| 2025년 6월 30일 | [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다. | Security Hub CSPM은 NIST SP 800-171 개정 2 표준에서 이 제어를 제거했습니다. NIST SP 800-171 개정 2는 90일 이하의 암호 만료 기간을 명시적으로 요구하지 않습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 6월 30일 | [RDS.16] Aurora DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다. | Security Hub CSPM은 이 제어의 제목을 변경했습니다. 새 제목은 제어가 Amazon Aurora DB 클러스터만 확인함을 보다 정확하게 반영합니다. 이전에는 이 제어의 제목이 RDS DB clusters should be configured to copy tags to snapshots였습니다. |
| 2025년 6월 30일 | [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다 | 이 제어는 Amazon SageMaker AI 노트북 인스턴스에 지정된 플랫폼 식별자를 기반으로 노트북 인스턴스가 지원되는 플랫폼에서 실행되도록 구성되어 있는지 확인합니다. Security Hub CSPM은 이 제어의 파라미터 값으로 `notebook-al2-v1` 및 `notebook-al2-v2`를 더 이상 지원하지 않습니다. 이러한 플랫폼에서 실행되는 노트북 인스턴스는 2025년 6월 30일에 지원이 종료되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 5월 30일 | [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다. | Security Hub CSPM은 PCI DSS v4.0.1 표준에서 이 제어를 제거했습니다. 이 제어는 IAM 사용자의 계정 암호 정책이 최소 암호 길이 7자를 포함한 최소 요구 사항을 충족하는지 확인합니다. PCI DSS v4.0.1은 이제 최소 암호 길이로 8자를 요구합니다. 암호 요구 사항이 다른 PCI DSS v3.2.1 표준에는 이 제어가 계속 적용됩니다.<br><br>PCI DSS v4.0.1 요구 사항을 기준으로 계정 암호 정책을 평가하려면 IAM.7 제어를 사용할 수 있습니다. 이 제어는 최소 암호 길이로 8자를 요구합니다. 또한 암호 길이 및 기타 파라미터에 대한 사용자 지정 값도 지원합니다. IAM.7 제어는 Security Hub CSPM의 PCI DSS v4.0.1 표준의 일부입니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 5월 8일 | [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다 | Security Hub CSPM은 모든 AWS 리전에서 RDS.46 제어 릴리스를 롤백했습니다. 이전에는이 제어가 AWS 기본 보안 모범 사례(FSBP) 표준을 지원했습니다. |
| 2025년 4월 7일 | [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다 | 이 제어는 Application Load Balancer의 HTTPS 리스너 또는 Network Load Balancer의 TLS 리스너가 권장 보안 정책을 사용하여 전송 중 데이터를 암호화하도록 구성되어 있는지 확인합니다. Security Hub CSPM은 이제 이 제어의 추가 파라미터 값 `ELBSecurityPolicy-TLS13-1-2-Res-2021-06` 및 `ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04` 를 지원합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 3월 27일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | 이 제어는 런타임에 대한 AWS Lambda 함수의 런타임 설정이 각 언어의 지원되는 최신 런타임에 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제이 컨트롤에 대한 파라미터 값으로 `ruby3.4`를 지원합니다.이 런타임에 대한 지원이 AWS Lambda 추가되었습니다. |
| 2025년 3월 26일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터가 지원되는 Kubernetes 버전에서 실행되고 있는지 여부를 확인합니다. `oldestVersionSupported` 파라미터의 경우 Security Hub CSPM은 값을 `1.29`에서 `1.30`으로 변경했습니다. 현재 지원되는 Kubernetes 버전 중 가장 오래된 버전은 `1.30`입니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 3월 10일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | 이 제어는 런타임에 대한 AWS Lambda 함수의 런타임 설정이 각 언어의 지원되는 최신 런타임에 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 더 이상이 제어에 대한 `python3.8` 파라미터 값으로 `dotnet6` 및를 지원하지 않습니다.는 더 이상 이러한 런타임을 지원하지 AWS Lambda 않습니다. |
| 2025년 3월 7일 | [RDS.18] RDS 인스턴스는 VPC에 배포되어야 합니다. | Security Hub CSPM은 AWS 기본 보안 모범 사례 표준 및 NIST SP 800-53 개정 5 요구 사항에 대한 자동 검사에서이 제어를 제거했습니다. Amazon EC2-Classic 네트워킹이 사용 중지되었으므로 Amazon Relational Database Service(Amazon RDS) 인스턴스는 더 이상 VPC 외부에 배포할 수 없습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2025년 1월 10일 | [Glue.2] AWS Glue 작업에는 로깅이 활성화되어 있어야 합니다. | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. |
| 2024년 12월 20일 | EC2.61~EC2.169 | Security Hub CSPM은 EC2.61~EC2.169 제어 릴리스를 롤백했습니다. |
| 2024년 12월 12일 | [RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다. | RDS.23은 Amazon Relational Database Service(Amazon RDS) 클러스터 또는 인스턴스가 데이터베이스 엔진의 기본 포트가 아닌 다른 포트를 사용하는지 확인합니다. 기본 AWS Config 규칙이 클러스터의 일부인 RDS 인스턴스에 `NOT_APPLICABLE` 대한 결과를 반환하도록 제어를 업데이트했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 12월 2일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `nodejs22.x` 를 파라미터로 지원합니다. |
| 2024년 11월 26일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터가 지원되는 Kubernetes 버전에서 실행되고 있는지 여부를 확인합니다. 현재 지원되는 버전 중 가장 오래된 버전은 `1.29`입니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 11월 20일 | [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. | Config.1은 AWS Config 가 활성화되었는지 확인하고, 서비스 연결 역할을 사용하고, 활성화된 제어에 대한 리소스를 기록합니다. Security Hub CSPM은 이 제어의 심각도를 `MEDIUM`에서 `CRITICAL`로 상향했습니다. 또한 Security Hub CSPM은 실패한 Config.1 조사 결과에 대한 새로운 상태 코드 및 상태 이유를 추가했습니다. 이러한 변경 사항은 Security Hub CSPM 제어 운영에서 Config.1의 중요성을 반영합니다. AWS Config 또는 리소스 기록이 비활성화된 경우 부정확한 제어 조사 결과를 받을 수 있습니다.<br><br>Config.1에 대한 `PASSED` 조사 결과를 수신하려면 활성화된 Security Hub CSPM 제어에 해당하는 리소스에 대한 리소스 기록을 켜고 조직에서 필요하지 않은 제어를 비활성화하세요. Security |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| | | Hub CSPM에 AWS Config 대한 구성에 대한 지침은 섹션을 참조하세요Security Hub CSPM AWS Config 에 대한 활성화 및 구성. Security Hub CSPM 제어 및 해당 리소스의 목록은 제어 조사 결과에 필요한 AWS Config리소스 섹션을 참조하세요. |
| 2024년 11월 12일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `python3.13` 를 파라미터로 지원합니다. |
| 2024년 10월 11일 | ElastiCache 제어 | ElastiCache.3, ElastiCache.4, ElastiCache.5, and ElastiCache.7의 제어 제목이 변경되었습니다. 제어는 ElastiCache for Valkey에도 적용되므로 제목은 더 이상 Redis OSS를 언급하지 않습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 9월 27일 | [ELB.4] Application Load Balancer는 잘못된 http 헤더를 삭제하도록 구성되어야 합니다. | 제어 제목이 Application Load Balancer는 http 헤더를 삭제하도록 구성되어야 합니다에서 Application Load Balancer는 유효하지 않은 http 헤더를 삭제하도록 구성되어야 합니다로 변경되었습니다. |
| 2024년 8월 19일 | DMS.12 및 ElastiCache 제어의 제목 변경 | ElastiCache.7을 통해 DMS.12 및 ElastiCache.1의 제어 제목이 변경되었습니다. Amazon ElastiCache(Redis OSS) 서비스의 이름 변경을 반영하도록 이 제목을 변경했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 8월 15일 | [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. | Config.1은 AWS Config 가 활성화되었는지 확인하고, 서비스 연결 역할을 사용하고, 활성화된 제어에 대한 리소스를 기록합니다. Security Hub CSPM은 `includeConfigServiceLinkedRoleCheck` 라는 사용자 지정 제어 파라미터를 추가했습니다. 이 파라미터를 `false`(으)로 설정하면 AWS Config 이(가) 서비스 연결 역할을 사용하는지 여부를 확인하지 않도록 선택할 수 있습니다. |
| 2024년 7월 31일 | [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다. | AWS IoT Core 보안 프로파일에서 변경된 제어 제목은 AWS IoT Device Defender 보안 프로파일은 태그 지정되어야 합니다로 을 태그 지정해야 합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 7월 29일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 더 이상 `nodejs16.x` 를 파라미터로 지원하지 않습니다. |
| 2024년 7월 29일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터가 지원되는 Kubernetes 버전에서 실행되고 있는지 여부를 확인합니다. 현재 지원되는 버전 중 가장 오래된 버전은 `1.28`입니다. |
| 2024년 6월 25일 | [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. | 이 제어는 AWS Config 가 활성화되어 있는지 확인하고, 서비스 연결 역할을 사용하고, 활성화된 제어에 대한 리소스를 기록합니다. Security Hub CSPM은 제어가 평가하는 내용을 반영하도록 제어 제목을 업데이트했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 6월 14일 | [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다. | 이 제어는 Amazon Aurora MySQL DB 클러스터가 Amazon CloudWatch Logs에 감사 로그를 게시하는지 여부를 확인합니다. Security Hub CSPM은 Aurora Serverless v1 DB 클러스터에 대한 조사 결과를 생성하지 않도록 제어를 업데이트했습니다. |
| 2024년 6월 11일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | 이 제어는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터가 지원되는 Kubernetes 버전에서 실행되고 있는지 여부를 확인합니다. 현재 지원되는 버전 중 가장 오래된 버전은 `1.27`입니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 6월 10일 | [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. | 이 제어는 AWS Config 가 활성화되어 있고 AWS Config 리소스 레코딩이 켜져 있는지 확인합니다. 이전에는 모든 리소스에 대해 기록을 구성한 경우에만 제어에서 PASSED 조사 결과를 생성했습니다. Security Hub CSPM 은 활성화된 제어에 필요한 리소스에 대해 기록이 켜져 있을 때 PASSED 조사 결과를 생성하도록 제어를 업데이트했습니다. 또한 필요한 리소스를 기록할 수 있는 권한을 제공하는 AWS Config 서비스 연결 역할이 사용되는지 여부를 확인하기 위해 제어가 업데이트되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 5월 8일 | [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다. | 이 제어는 Amazon S3 범용 버전 버킷에서 다중 인증(MFA) 삭제가 활성화되었는지 여부를 확인합니다. 이전에는 제어에서 수명 주기 구성이 있는 버킷에 대한 FAILED 조사 결과를 생성했습니다. 그러나 수명 주기 구성이 있는 버킷에서는 버전 관리가 있는 MFA 삭제를 활성화할 수 없습니다. Security Hub CSPM은 수명 주기 구성이 있는 버킷에 대한 조사 결과를 생성하지 않도록 제어를 업데이트했습니다. 제어 기능의 설명이 현재 동작을 반영하도록 업데이트되었습니다. |
| 2024년 5월 2일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | Security Hub CSPM은 통과된 조사 결과를 생성하기 위해 Amazon EKS 클러스터를 실행할 수 있도록 지원하는 Kubernetes의 가장 오래된 버전을 업데이트했습니다. 현재 지원되는 버전 중 가장 오래된 버전은 Kubernetes 1.26입니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 4월 30일 | [CloudTrail.3] 하나 이상의 CloudTrail 추적을 활성화해야 합니다. | 제어 제목이 CloudTrail을 활성화해야 합니다에서 최소 CloudTrail 추적을 활성화해야 합니다로 변경되었습니다. 이 제어는 현재에 하나 이상의 CloudTrail 추적 AWS 계정 이 활성화된 경우 PASSED 결과를 생성합니다. 현재 동작을 정확하게 반영하도록 제목과 설명이 변경되었습니다. |
| 2024년 4월 29일 | [PCI.AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다. | 제어 제목이 Classic Load Balancer와 연결된 Auto Scaling 그룹은 로드 밸런서 상태 확인을 사용해야 합니다에서 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다로 변경되었습니다. 이 제어는 현재 Application, Gateway, Network 및 Classic Load Balancer를 평가합니다. 현재 동작을 정확하게 반영하도록 제목과 설명이 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 4월 19일 | [CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다. | 제어는 AWS CloudTrail 가 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어 있는지 확인합니다. 이전에는 추적이 읽기 및 쓰기 관리 이벤트를 캡처하지 않았더라도, 계정에 CloudTrail이 활성화되고 하나 이상의 다중 리전 추적으로 구성된 경우, 제어에서 PASSED 조사 결과가 잘못 생성되었습니다. 이제 제어는 CloudTrail가 활성화되고 읽기 및 쓰기 관리 이벤트를 캡처하는 다중 리전 추적이 하나 이상 구성된 경우에만 PASSED 조사 결과를 생성합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 4월 10일 | [Athena.1] Athena 워크그룹은 저장 시 암호화되어야 합니다 | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. Athena 작업 그룹은 Amazon Simple Storage Service(Amazon S3) 버킷에 로그를 전송합니다. Amazon S3는 이제 새로운 및 기존 S3 버킷에 S3 관리형 키(SS3-S3)를 사용한 기본 암호화를 제공합니다. |
| 2024년 4월 10일 | [AutoScaling.4] Auto Scaling 그룹 시작 구성에는 1보다 큰 메타데이터 응답 홉 제한이 있어서는 안 됩니다 | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 메타데이터 응답 홉 제한은 워크로드에 따라 다릅니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 4월 10일 | [CloudFormation.1] CloudFormation 스택은 SNS(Simple Notification Service)와 통합 | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. AWS CloudFormation 스택을 Amazon SNS 주제와 통합하는 것은 더 이상 보안 모범 사례가 아닙니다. 중요한 CloudFormation 스택을 SNS 주제와 통합하는 것이 유용할 수 있지만 모든 스택에 필요한 것은 아닙니다. |
| 2024년 4월 10일 | [CodeBuild.5] CodeBuild 프로젝트 환경에서는 권한 모드가 활성화되어서는 안 됩니다 | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. CodeBuild 프로젝트에서 권한 있는 모드를 활성화해도 고객 환경에 추가 위험이 발생하지 않습니다. |
| 2024년 4월 10일 | [IAM.20] 루트 사용자의 사용을 피합니다 | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. 이 제어의 목적은 다른 제어인 [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다.에서 다룹니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 4월 10일 | [SNS.2] 주제에 전송된 알림 메시지에 대해 전송 상태 로깅이 활성화되어야 합니다 | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. SNS 주제에 대한 전송 상태 로깅은 더 이상 보안 모범 사례가 아닙니다. 중요한 SNS 주제에 대한 전송 상태 로깅이 유용할 수 있지만 모든 주제에 필요한 것은 아닙니다. |
| 2024년 4월 10일 | [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다 | Security Hub CSPM은 AWS 기본 보안 모범 사례 및 서비스 관리형 표준에서이 제어를 제거했습니다 AWS Control Tower. 이 제어의 목적은 두 가지 다른 제어인 [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다 및 [S3.14] S3 범용 버킷에는 버전 관리가 활성화되어 있어야 합니다에서 다룹니다. 이 제어는 여전히 NIST SP 800-53 개정판 5에 포함됩니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 4월 10일 | [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다 | Security Hub CSPM은 AWS 기본 보안 모범 사례 및 서비스 관리형 표준에서이 제어를 제거했습니다 AWS Control Tower. S3 버킷에 대한 이벤트 알림이 유용한 경우가 있지만, 이는 범용 보안 모범 사례는 아닙니다. 이 제어는 여전히 NIST SP 800-53 개정판 5에 포함됩니다. |
| 2024년 4월 10일 | [SNS.1] SNS 주제는를 사용하여 유휴 시 암호화되어야 합니다.AWS KMS | Security Hub CSPM은 AWS 기본 보안 모범 사례 및 서비스 관리형 표준에서이 제어를 제거했습니다 AWS Control Tower. 기본적으로 SNS는 디스크 암호화를 통해 저장 중인 주제를 암호화합니다. 자세한 내용은 데이터 암호화를 참조하세요. AWS KMS 를 사용하여 주제를 암호화하는 것은 더 이상 보안 모범 사례로 권장되지 않습니다. 이 제어는 여전히 NIST SP 800-53 개정판 5에 포함됩니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 4월 8일 | [ELB.6] 애플리케이션, 게이트웨이, Network Load Balancers에는 삭제 보호가 활성화되어 있어야 합니다. | 제어 제목이 Application Load Balancer 삭제 방지를 활성화해야 합니다에서 Application, Gateway 및 Network Load Balancer 삭제 방지가 활성화되어 있어야 합니다로 변경되었습니다. 이 제어는 현재 Application, Gateway 및 Network Load Balancer를 평가합니다. 현재 동작을 정확하게 반영하도록 제목과 설명이 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 22일 | [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다. | 제어 제목이 OpenSearch 도메인에 대한 연결은 TLS 1.2를 사용하여 암호화해야 합니다에서 OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다로 변경되었습니다. 이전에는 컨트롤이 OpenSearch 도메인에 대한 연결에 TLS 1.2가 사용되었는지만 확인했습니다. 이제 제어는 OpenSearch 도메인이 최신 TLS 보안 정책을 사용하여 암호화되는 경우, PASSED 조사 결과를 생성합니다. 제어 기능의 제목과 설명이 현재 동작을 반영하도록 업데이트되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 22일 | [ES.8] Elasticsearch 도메인에 대한 연결은 TLS 보안 정책을 사용하여 암호화해야 합니다. | 제어 제목이 Elasticsearch 도메인에 대한 연결은 TLS 1.2를 사용하여 암호화되어야 합니다에서 Elasticsearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다로 변경되었습니다. 이전에는 제어가 Elasticsearch 도메인에 대한 연결에 TLS 1.2가 사용되었는지 여부만 확인했습니다. 이제 제어는 Elasticsearch 도메인이 최신 TLS 보안 정책을 사용하여 암호화되는 경우, PASSED 조사 결과를 생성합니다. 제어 기능의 제목과 설명이 현재 동작을 반영하도록 업데이트되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 12일 | [S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다 | 제목이 S3 퍼블릭 액세스 차단 설정이 활성화되어야 합니다에서 S3 범용 버킷에는 공개 액세스 차단 설정이 활성화되어 있어야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다. | 제목이 S3 버킷은 공개 읽기 액세스를 금지해야 합니다에서 S3 범용 버킷은 공개 읽기 액세스를 차단해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다 | 제목이 S3 버킷은 공개 쓰기 액세스를 금지해야 합니다에서 S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 12일 | [S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다. | 제목이 S3 버킷에는 보안 소켓 계층(Secure Socket Layer) 사용 요청이 필요합니다에서S3 범용 버킷에는 SSL 사용 요청이 필요합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.6] S3 범용 버킷 정책은 다른에 대한 액세스를 제한해야 합니다. AWS 계정 | 제목이 버킷 정책에서 다른 AWS 계정 에 부여된 S3 권한을 제한해야 합니다에서 S3 범용 버킷 정책은 다른 AWS 계정에 대한 액세스를 제한해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 12일 | [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다 | 제목이 S3 버킷은 리전 간 복제가 활성화되어 있어야 합니다에서 S3 범용 버킷은 리전 간 복제를 사용해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다 | 제목이 S3 버킷은 리전 간 복제가 활성화되어 있어야 합니다에서 S3 범용 버킷은 리전 간 복제를 사용해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다. | 제목이 S3 공개 액세스 차단 설정이 버킷 수준에서 활성화되어야 합니다에서 S3 범용 버킷은 공개 액세스를 차단해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 12일 | [S3.9] S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다 | 제목이 S3 버킷 서버 액세스 로깅이 활성화되어야 합니다에서 S3 범용 버킷에 대해 서버 액세스 로깅을 활성화해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다 | 제목이 버전 관리가 활성화된 S3 버킷에는 수명 주기 정책이 구성되어 있어야 합니다 에서 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 12일 | [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다 | 제목이 S3 버킷에는 이벤트 알림이 활성화되어 있어야 합니다에서 S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다 | 제목이 버킷에 대한 사용자 액세스를 관리하는 데 S3 액세스 제어 목록(ACLs)를 사용해서는 안 됩니다에서 S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 12일 | [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다 | 제목이 S3 버킷에는 수명 주기 정책이 구성되어 있어야 합니다에서 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.14] S3 범용 버킷에는 버전 관리가 활성화되어 있어야 합니다 | 제목이 S3 버킷은 버전 관리를 사용해야 합니다에서 S3 범용 버킷에서는 버전 관리를 활성화해야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 12일 | [S3.15] S3 범용 버킷에는 Object Lock이 활성화되어 있어야 합니다. | 제목이 S3 버킷이 Object Lock을 사용하도록 구성해야 합니다에서 S3 범용 버킷에는 Object Lock이 활성화되어 있어야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 3월 12일 | [S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys | 제목이 S3 버킷은 저장 시 AWS KMS keys 로 암호화되어야 합니다에서 S3 범용 버킷은 저장 시 AWS KMS keys로 암호화되어야 합니다로 변경되었습니다. Security Hub CSPM은 새로운 S3 버킷 유형을 설명하도록 제목을 변경했습니다. |
| 2024년 3월 7일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `nodejs20.x` 및 `ruby3.3`을 파라미터로 지원합니다. |
| 2024년 2월 22일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `dotnet8`를 파라미터로 지원합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 2월 5일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | Security Hub CSPM은 통과된 조사 결과를 생성하기 위해 Amazon EKS 클러스터를 실행할 수 있도록 지원하는 Kubernetes의 가장 오래된 버전을 업데이트했습니다. 현재 지원되는 버전 중 가장 오래된 버전은 Kubernetes `1.25`입니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 1월 10일 | [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다. | 제목이 CodeBuild GitHub 또는 Bitbucket 소스 리포지토리 URL은 OAuth를 사용해야 합니다에서 CodeBuild Bitbucket 소스 리포지토리 URL은 민감한 보안 인증 정보를 포함하지 않아야 합니다로 변경되었습니다. 다른 연결 방법도 안전할 수 있으므로 Security Hub CSPM은 OAuth에 대한 언급을 제거했습니다. GitHub 소스 리포지토리 URL에 개인 액세스 토큰 또는 사용자 이름과 암호를 더 이상 가질 수 없으므로 Security Hub CSPM은 GitHub에 대한 언급을 제거했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2024년 1월 8일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 더 이상 `go1.x` 및 `java8`를 파라미터로 지원하지 않습니다. 사용 중지된 런타임이기 때문입니다. |
| 2023년 12월 29일 | [RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다. | RDS.8은 지원되는 데이터베이스 엔진 중 하나를 사용하는 Amazon RDS DB 인스턴스에 삭제 보호가 활성화되어 있는지 확인합니다. Security Hub CSPM은 이제 `custom-oracle-ee`, `oracle-ee-cdb` 및 `oracle-se2-cdb` 를 데이터베이스 엔진으로 지원합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 12월 22일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `java21` 및 `python3.12` 을 파라미터로 지원합니다. Security Hub CSPM은 더 이상 `ruby2.7`를 파라미터로 지원하지 않습니다. |
| 2023년 12월 15일 | [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다. | CloudFront.1은 Amazon CloudFront 배포에 기본 루트 객체가 구성되어 있는지 확인합니다. Security Hub CSPM은 기본 루트 객체를 추가하는 것이 사용자의 애플리케이션 및 특정 요구 사항에 따라 달라지는 권장 사항이기 때문에 이 제어의 심각도를 심각에서 높음으로 낮췄습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 12월 5일 | [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다. | 제어 기능의 제목이 보안 그룹은 0.0.0.0/0에서 포트 22로의 수신을 허용하지 않아야 합니다에서 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용하지 않아야 합니다로 변경되었습니다. |
| 2023년 12월 5일 | [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다. | 제어 기능의 제목이 0.0.0.0/0에서 포트 3389로의 수신을 허용하는 보안 그룹이 없는지 확인합니다에서 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용하지 않아야 합니다로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 12월 5일 | [RDS.9] RDS DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다. | 제어 기능의 제목이 데이터베이스 로깅을 활성화해야 합니다에서 RDS DB 인스턴스는 CloudWatch Logs에 로그를 게시해야 합니다로 변경되었습니다. Security Hub CSPM 은 이 제어는 로그가 Amazon CloudWatch Logs에 게시되었는지 여부만 확인하고 RDS 로그가 활성화되었는지 여부는 확인하지 않는다는 것을 식별했습니다. 이 제어는 RDS DB 인스턴스가 CloudWatch Logs에 로그를 게시하도록 구성된 경우, PASSED 조사 결과를 생성합니다. 제어 기능의 제목이 현재 동작을 반영하여 업데이트되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 12월 5일 | [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다. | 이 제어는 Amazon EKS 클러스터에 감사 로깅이 활성화되어 있는지 여부를 확인합니다. Security Hub CSPM이 이 제어를 평가하는 데 사용하는 AWS Config 규칙이에서 `eks-cluster-logging-enabled` 로 변경되었습니다`eks-cluster-log-enabled` . |
| 2023년 11월 17일 | [EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다. | EC2.19가 보안 그룹에 대한 무제한 수신 트래픽이 위험이 높다고 간주되는 지정된 포트에 액세스할 수 있는지 여부를 확인합니다. Security Hub CSPM은 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 이 제어를 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우, `FAILED` 조사 결과를 생성합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 11월 16일 | [CloudWatch.15] CloudWatch 경보에는 지정된 구성되어 있어야 합니다. | 제어 기능의 제목이 CloudWatch 경보에는 경보 상태에 맞게 구성된 작업이 있어야 합니다에서 CloudWatch 경보에는 지정된 작업이 구성되어야 합니다로 변경되었습니다. |
| 2023년 11월 16일 | [CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다. | 제어 기능의 제목이 CloudWatch 로그 그룹은 최소 1년 동안 보존되어야 합니다에서 CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다로 변경되었습니다. |
| 2023년 11월 16일 | [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다. | 제어 기능의 제목이 VPC Lambda 함수는 두 개 이상의 가용 영역에서 작동해야 합니다에서 VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 11월 16일 | [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다. | 제어 기능의 제목이 AWS AppSync 는 request-level 및 field-level 로깅을 활성화된 상태로 두어야 합니다에서 AWS AppSync 는 field-level 로깅을 활성화된 상태로 두어야 합니다로 변경되었습니다. |
| 2023년 11월 16일 | [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다. | 제어 기능의 제목이 Amazon Elastic MapReduce 클러스터 마스터 노드에는 퍼블릭 IP 주소가 없어야 합니다에서 Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다로 변경되었습니다. |
| 2023년 11월 16일 | [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다. | 제어 기능의 제목이 OpenSearch 도메인은 VPC에 있어야 합니다에서 OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 11월 16일 | [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다. | 제어 기능의 제목이 Elasticsearch 도메인은 VPC에 있어야 합니다에서 Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 10월 31일 | [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다. | ES.4가 Elasticsearch 도메인이 오류 로그를 Amazon CloudWatch Logs로 전송하도록 구성되어 있는지 여부를 확인합니다. 이 제어 기능은 이전에 CloudWatch Logs로 전송하도록 구성된 모든 로그를 보유하고 있는 Elasticsearch 도메인에 대한 PASSED 조사 결과를 생성했습니다. Security Hub CSPM은 오류 로그를 CloudWatch Logs로 전송하도록 구성된 Elasticsearch 도메인에 대한 PASSED 조사 결과만 생성하도록 제어를 업데이트했습니다. 또한, 오류 로그를 지원하지 않는 Elasticsearch 버전을 평가에서 제외하도록 제어 기능을 업데이트했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 10월 16일 | [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다. | EC2.13은 보안 그룹이 포트 22에 대한 무제한 수신 액세스를 허용하는지 확인합니다. Security Hub CSPM은 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 이 제어를 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우 FAILED 결과를 생성합니다. |
| 2023년 10월 16일 | [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다. | EC2.14는 보안 그룹이 포트 3389에 대한 무제한 수신 액세스를 허용하는지 확인합니다. Security Hub CSPM은 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 이 제어를 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우 FAILED 결과를 생성합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 10월 16일 | [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다. | EC2.18은 사용 중인 보안 그룹이 무제한 수신 트래픽을 허용하는지 여부를 확인합니다. Security Hub CSPM은 관리형 접두사 목록이 보안 그룹 규칙의 원본으로 제공될 때 이를 반영하도록 이 제어를 업데이트했습니다. 이 제어는 접두사 목록에 '0.0.0.0/0' 또는 '::/0' 문자열이 포함된 경우 FAILED 결과를 생성합니다. |
| 2023년 10월 16일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 python3.11 를 파라미터로 지원합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 10월 4일 | [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다 | Security Hub CSPM은 S3 버킷에서 동일 리전 복제 대신 리전 간 복제가 활성화되도록 하기 위해 값이 `CROSS-REGION` 인 파라미터 `ReplicationType` 을 추가했습니다. |
| 2023년 9월 27일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | Security Hub CSPM은 통과된 조사 결과를 생성하기 위해 Amazon EKS 클러스터를 실행할 수 있도록 지원하는 Kubernetes의 가장 오래된 버전을 업데이트했습니다. 현재 지원되는 버전 중 가장 오래된 버전은 Kubernetes `1.24`입니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 9월 20일 | [CloudFront.2] CloudFront 배포에는 오리진 액세스 ID가 활성화되어 있어야 합니다. | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. 대신 [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다. 섹션을 참조하세요. 원본 액세스 제어 기능은 현재 보안 모범 사례입니다. 이 제어는 90일 후에 설명서에서 제거됩니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 9월 20일 | [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다. | Security Hub CSPM은 AWS Foundational Security Best Practices(FSBP) 및 National Institute of Standards and Technology(NIST) SP 800-53 Rev. 5에서이 제어를 제거했습니다. 여전히 서비스 관리형 표준:의 일부입니다 AWS Control Tower. 이 제어는 보안 그룹이 EC2 인스턴스 또는 탄력적 네트워크 인터페이스에 연결된 경우, 통과된 조사 결과를 생성합니다. 하지만, 특정 사용 사례에 대해서는 연결되지 않은 보안 그룹이 보안 위험을 초래하지는 않습니다. EC2.2, EC2.13, EC2.14, EC2.18, EC2.19 등의 다른 EC2 제어를 사용하여 보안 그룹을 모니터링할 수 있습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 9월 20일 | [EC2.29] EC2 인스턴스는 VPC에서 시작해야 합니다. | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. Amazon EC2는 EC2-Classic 인스턴스를 VPC로 마이그레이션했습니다. 이 제어는 90일 후에 설명서에서 제거됩니다. |
| 2023년 9월 20일 | [S3.4] S3 버킷에는 서버 측 암호화가 활성화되어 있어야 합니다. | Security Hub CSPM은 이 제어를 사용 중지했고 모든 표준에서 제거했습니다. Amazon S3는 이제 새로운 및 기존 S3 버킷에 S3 관리형 키(SS3-S3)를 사용한 기본 암호화를 제공합니다. SS3-S3 또는 SS3-KMS 서버 측 암호화로 암호화된 기존 버킷의 암호화 설정은 변경되지 않습니다. 이 제어는 90일 후에 설명서에서 제거됩니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 9월 14일 | [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다. | 제어 기능의 제목이 VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됨에서 VPC 기본 보안 그룹들은 인바운드 또는 아웃바운드 트래픽을 허용해서는 안 됨으로 변경되었습니다. |
| 2023년 9월 14일 | [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다. | 제어 기능의 제목이 가상 MFA는 루트 사용자에 대해 활성화되어야 함에서 MFA는 루트 사용자에 대해 활성화되어야 함으로 변경되었습니다. |
| 2023년 9월 14일 | [RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다. | 제어 기능의 제목이 중요 클러스터 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 함에서 중요 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 함으로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 9월 14일 | [RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다. | 제어 기능의 제목이 중요 데이터베이스 인스턴스 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 함에서 중요 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 함으로 변경되었습니다. |
| 2023년 9월 14일 | [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다. | 제어 기능의 제목이 WAF 리전 규칙에는 하나 이상의 조건이 있어야 함에서 AWS WAF 클래식 리전 규칙에는 하나 이상의 조건이 있어야 함으로 변경되었습니다. |
| 2023년 9월 14일 | [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다. | 제어 기능의 제목이 WAF 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 함에서 AWS WAF 클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 함으로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 9월 14일 | [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다. | 제어 기능의 제목이 WAF 리전 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함에서 AWS WAF 클래식 리전 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함으로 변경되었습니다. |
| 2023년 9월 14일 | [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다. | 제어 기능의 제목이 WAF 전역 규칙에는 하나 이상의 조건이 있어야 함에서 AWS WAF 클래식 전역 규칙에는 하나 이상의 조건이 있어야 함으로 변경되었습니다. |
| 2023년 9월 14일 | [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다. | 제어 기능이 제목이 WAF 전역 규칙 그룹에는 하나 이상의 규칙이 있어야 함에서 AWS WAF 클래식 전역 규칙 그룹에는 하나 이상의 규칙이 있어야 함으로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 9월 14일 | [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다. | 제어 기능의 제목이 WAF 전역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함에서 AWS WAF 클래식 전역 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함으로 변경되었습니다. |
| 2023년 9월 14일 | [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다. | 제어 기능의 제목이 WAFv2 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함에서 AWS WAF 웹 ACL에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 함으로 변경되었습니다. |
| 2023년 9월 14일 | [WAF.11]AWS WAF웹 ACL 로깅을 활성화해야 합니다. | 제어 기능의 제목이 AWS WAF v2 웹 ACL 로깅을 활성화해야 함에서 AWS WAF 웹 ACL 로깅을 활성화해야 함으로 변경되었습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 7월 20일 | [S3.4] S3 버킷에는 서버 측 암호화가 활성화되어 있어야 합니다. | S3.4는 Amazon S3 버킷에 서버 측 암호화가 활성화되어 있는지 또는 S3 버킷 정책이 서버 측 암호화되지 않은 `PutObject` 요청을 명시적으로 거부하는지 확인합니다. Security Hub CSPM은 KMS 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)를 포함하도록 이 제어를 업데이트했습니다. 이 제어 기능은 S3 버킷이 SSE-S3, SSE-KMS 또는 DSSE-KMS로 암호화될 때 통과된 조사 결과를 생성합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 7월 17일 | [S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys | S3.17은 Amazon S3 버킷이 AWS KMS key 을(를) 사용하여 암호화되었는지 여부를 확인합니다. Security Hub CSPM은 KMS 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)를 포함하도록 이 제어를 업데이트했습니다. 이 제어 기능은 S3 버킷이 SSE-KMS 또는 DSSE-KMS로 암호화될 때 통과된 조사 결과를 생성합니다. |
| 2023년 6월 9일 | [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다. | EKS.2는 Amazon EKS 클러스터가 지원되는 Kubernetes 버전에서 실행되고 있는지 확인합니다. 현재 지원되는 가장 오래된 버전은 `1.23`입니다. |
| 2023년 6월 9일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `ruby3.2`를 파라미터로 지원합니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 6월 5일 | [APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다. | APIGateway.5.는 Amazon API Gateway REST API 스테이지의 모든 메서드가 저장 시 암호화되어 있는지 확인합니다. Security Hub CSPM은 특정 메서드에 대해 캐싱이 활성화된 경우에만 해당 메서드의 암호화를 평가하도록 제어를 업데이트했습니다. |
| 2023년 5월 18일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `java17`를 파라미터로 지원합니다. |
| 2023년 5월 18일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 더 이상 `nodejs12.x` 를 파라미터로 지원하지 않습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 4월 23일 | [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다. | ECS.10은 Amazon ECS Fargate 서비스가 최신 Fargate 플랫폼 버전을 실행하고 있는지 여부를 확인합니다. 고객은 ECS를 통해 직접 또는 CodeDeploy를 사용하여 Amazon ECS를 배포할 수 있습니다. Security Hub CSPM은 CodeDeploy를 사용하여 ECS Fargate 서비스를 배포할 때 통과됨 조사 결과를 생성하도록 이 제어를 업데이트했습니다. |
| 2023년 4월 20일 | [S3.6] S3 범용 버킷 정책은 다른에 대한 액세스를 제한해야 합니다. AWS 계정 | S3.6은 Amazon Simple Storage Service(Amazon S3) 버킷 정책이 다른 보안 주체가 S3 버킷의 리소스에 대해 거부된 작업을 AWS 계정 수행하지 못하도록 하는지 확인합니다. Security Hub CSPM은 버킷 정책에서 조건문을 반영하도록 제어를 업데이트했습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 4월 18일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 이제 `python3.10` 를 파라미터로 지원합니다. |
| 2023년 4월 18일 | [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다. | Lambda.2는 런타임에 대한 AWS Lambda 함수 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Security Hub CSPM은 더 이상 `dotnetcore3.1` 를 파라미터로 지원하지 않습니다. |

| 변경 날짜 | 제어 ID 및 제목 | 변경 내용 설명 |
| --- | --- | --- |
| 2023년 4월 17일 | [RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다. | RDS.11은 Amazon RDS 인스턴스에 백업 보존 기간이 7일 이상인 자동 백업이 활성화되어 있는지 여부를 확인합니다. 모든 엔진이 읽기 전용 복제본의 자동 백업을 지원하는 것은 아니므로 Security Hub CSPM은 읽기 전용 복제본을 평가에서 제외하도록 이 제어를 업데이트했습니다. 또한, RDS는 읽기 전용 복제본을 생성할 때 백업 보존 기간을 지정하는 옵션을 제공하지 않습니다. 읽기 전용 복제본은 기본적으로 백업 보존 기간을 0(으)로 설정하여 생성됩니다. |

## 에 대한 Security Hub CSPM 제어AWS 계정

이러한 Security Hub CSPM 제어는를 평가합니다AWS 계정.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정

관련 요구 사항: CIS AWSFoundations Benchmark v5.0.0/1.2, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `security-account-information-provided`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Web Services(AWS) 계정에 보안 연락처 정보가 있는지 확인합니다. 계정에 대한 보안 연락처 정보가 제공되지 않으면 제어가 실패합니다.

대체 보안 연락처를 통해 AWS는 사용자 계정을 사용할 수 없는 경우 계정 관련 문제에 대해 다른 사람에게 연락할 수 있습니다. 지원또는 다른AWS 서비스 팀으로부터 AWS 계정사용량과 관련된 보안 관련 주제에 대한 알림을 받을 수 있습니다.

문제 해결

대체 연락처를 보안 연락처로에 추가하려면 AWS계정 관리 참조 안내서의에 대한 대체 연락처 업데이트를 AWS 계정참조하세요. AWS 계정

[Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.

범주: 보호 > 보안 액세스 관리 > 액세스 제어

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `account-part-of-organizations`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS 계정가를 통해 관리되는 조직의 일부인지 확인합니다AWS Organizations. 계정이 조직의 일부가 아닌 경우, 제어가 실패합니다.

Organizations를 사용하면 워크로드를 확장할 때 환경을 중앙에서 관리할 수 있습니다AWS. 특정 보안 요구 사항이 있는 워크로드를 격리하거나 HIPAA 또는 PCI와 같은 프레임워크를 준수하기 위해 여러 개의 AWS 계정을 사용할 수 있습니다. 조직을 생성하면 여러 계정을 단일 단위로 관리하고AWS 서비스, 리소스 및 리전에 대한 액세스를 중앙에서 관리할 수 있습니다.

문제 해결

새 조직을 생성하고 자동으로 추가하려면 AWS Organizations사용 설명서의 조직 생성을 참조AWS 계정하세요. 기존 조직에 계정을 추가하려면 AWS Organizations사용 설명서의 조직에 가입AWS 계정하도록 초대를 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Amplify

이러한 Security Hub CSPM 제어는 AWS Amplify서비스와 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Amplify.1] Amplify 앱에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Amplify::App`

AWS Config 규칙: amplify-app-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Amplify앱에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 앱에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 앱에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS Amplify앱에 태그를 추가하는 방법에 대한 자세한 내용은 호스팅 사용 설명서의 리소스 태그 지정 지원을 참조하세요. AWS Amplify

[Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Amplify::Branch`

AWS Config 규칙: amplify-branch-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Amplify브랜치에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 브랜치에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 브랜치에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS Amplify브랜치에 태그를 추가하는 방법에 대한 자세한 내용은 호스팅 사용 설명서의 리소스 태그 지정 지원을 참조하세요. AWS Amplify

## Amazon API Gateway에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon API Gateway 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[APIGateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`, `AWS::ApiGatewayV2::Stage`

AWS Config 규칙: api-gw-execution-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `loggingLevel` | 로깅 수준 | Enum | `ERROR`, `INFO` | `No default value` |

이 제어는 Amazon API Gateway REST 또는 WebSocket API의 모든 단계에서 로깅이 활성화되었는지 확인합니다. API의 모든 단계에 대해 `loggingLevel`이 `ERROR` 또는 `INFO`가 아니면 제어가 실패합니다. 특정 로그 유형을 활성화해야 함을 나타내는 사용자 지정 파라미터 값을 제공하지 않는 한, Security Hub CSPM은 로깅 수준이 `ERROR` 또는 인 경우 전달된 결과를 생성합니다`INFO`.

API Gateway REST 또는 WebSocket API 스테이지에는 관련 로그가 활성화되어 있어야 합니다. API Gateway REST 및 WebSocket API 실행 로깅은 API Gateway REST 및 WebSocket API 단계에 대한 요청의 세부 기록을 제공합니다. 단계에는 API 통합 백엔드 응답, Lambda 권한 부여자 응답 및 AWS 통합 엔드포인트`requestId`용가 포함됩니다.

문제 해결

REST 및 WebSocket API 작업에 대한 로깅을 활성화하려면 API Gateway 개발자 안내서의 API Gateway 콘솔을 사용하여 CloudWatch API 로깅 설정을 참조하세요.

[APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: api-gw-ssl-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon API Gateway REST API 단계에 SSL 인증서가 구성되어 있는지 여부를 확인합니다. 백엔드 시스템은 이러한 인증서를 사용하여 들어오는 요청이 API 게이트웨이에서 온 것임을 인증합니다.

API 게이트웨이 REST API 단계는 백엔드 시스템이 API 게이트웨이에서 발생한 요청을 인증할 수 있도록 SSL 인증서로 구성되어야 합니다.

문제 해결

API Gateway REST API SSL 인증서를 생성하고 구성하는 방법에 대한 자세한 지침은 API Gateway 개발자 안내서의 백엔드 인증을 위한 SSL 인증서 생성 및 구성을 참조하세요.

[APIGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: api-gw-xray-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon API Gateway REST API 단계에 활성 AWS X-Ray 추적이 활성화되어 있는지 확인합니다.

X-Ray 활성 추적을 통해 기본 인프라의 성능 변화에 보다 신속하게 대응할 수 있습니다. 성능 변화로 인해 API의 가용성이 떨어질 수 있습니다. X-Ray 활성 추적은 API Gateway REST API 작업 및 연결된 서비스를 통해 전달되는 사용자 요청의 실시간 메트릭를 제공합니다.

문제 해결

API Gateway REST API 작업에 대해 X-Ray 활성 추적을 활성화하는 방법에 대한 자세한 지침은 AWS X-Ray 개발자 안내서의 AWS X-Ray에 대한 Amazon API Gateway 활성 추적 지원을 참조하세요.

[APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21)

범주: 보호 > 보호 서비스

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: api-gw-associated-with-waf

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 API Gateway 단계에서 AWS WAF 웹 액세스 제어 목록(ACL)을 사용하는지 확인합니다. AWS WAF 웹 ACL이 REST API Gateway 단계에 연결되지 않은 경우이 제어가 실패합니다.

AWS WAF 는 웹 애플리케이션 및 APIs으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 이를 통해 사용자 정의 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 집합인 ACL을 구성할 수 있습니다. API Gateway 단계가 AWS WAF 웹 ACL과 연결되어 있는지 확인하여 악의적인 공격으로부터 보호합니다.

문제 해결

API Gateway 콘솔을 사용하여 AWS WAF 리전 웹 ACL을 기존 API Gateway API 단계와 연결하는 방법에 대한 자세한 내용은 APIs Gateway 개발자 안내서의 API 보호를 위한 사용을 AWS WAF 참조하세요.

[APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ApiGateway::Stage`

AWS Config 규칙: `api-gw-cache-encrypted` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 캐시가 활성화된 API Gateway REST API 단계의 모든 메서드가 암호화되었는지 여부를 확인합니다. API Gateway REST API 단계의 메서드가 캐시되도록 구성되어 있고 캐시가 암호화되지 않은 경우, 제어가 실패합니다. Security Hub CSPM은 해당 메서드에 대해 캐싱이 활성화된 경우에만 특정 메서드의 암호화를 평가합니다.

저장 데이터를 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다 AWS. 승인되지 않은 사용자의 데이터 액세스를 제한하기 위해 또 다른 액세스 제어 세트를 추가합니다. 예를 들어, 데이터를 읽기 전에 해독하려면 API 권한이 필요합니다.

API 게이트웨이 REST API 캐시는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다.

문제 해결

단계에 대한 API 캐싱을 구성하려면 API Gateway 개발자 안내서의 Amazon API Gateway 캐싱 활성화를 참조하세요. 캐시 설정에서 캐시 데이터 암호화를 선택합니다.

[APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::ApiGatewayV2::Route`

AWS Config 규칙: api-gwv2-authorization-type-configured

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `authorizationType` | API 경로의 권한 부여 유형 | Enum | `AWS_IAM`, `CUSTOM`, `JWT` | 기본값 없음 |

이 제어는 Amazon API Gateway 경로에 인증 유형이 있는지 확인합니다. 인증 유형이 API 게이트웨이 경로에 없으면 제어가 실패합니다. 필요에 따라, 경로가 파라미터에 지정된 인증 유형을 사용하는 경우에만 제어가 전달되도록 하려면 사용자 지정 `authorizationType` 파라미터 값을 제공할 수 있습니다.

API Gateway는 API 액세스 제어 및 관리에 다중 메커니즘을 지원합니다. 인증 유형을 지정하면 API에 대한 액세스를 인증된 사용자 또는 프로세스로만 제한할 수 있습니다.

문제 해결

HTTP API에 대한 인증 유형을 설정하려면 API Gateway 개발자 안내서의 API Gateway에서 HTTP API에 대한 액세스 제어 및 관리를 참조하세요. WebSocket API에 대한 권한 부여 유형을 설정하려면 API Gateway 개발자 안내서의 API Gateway에서 WebSocket API에 대한 액세스 제어 및 관리를 참조하세요.

[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ApiGatewayV2::Stage`

AWS Config 규칙: api-gwv2-access-logs-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon API Gateway V2 단계에 액세스 로깅이 구성되어 있는지 확인합니다. 액세스 로그 설정이 정의되지 않은 경우, 이 제어가 실패합니다.

API Gateway 액세스 로그는 누가 API에 액세스했고 호출자가 API에 어떻게 액세스했는지에 대한 자세한 정보를 제공합니다. 이러한 로그는 보안 및 액세스 감사 및 포렌식 조사와 같은 애플리케이션에 유용합니다. 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 문제를 해결할 수 있습니다.

추가 모범 사례는 API Gateway 개발자 안내서의 REST API 모니터링을 참조하세요.

문제 해결

액세스 로깅을 설정하려면 API Gateway 개발자 안내서의 API Gateway 콘솔을 사용하여 CloudWatch API 로깅 설정을 참조하세요.

[APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ApiGatewayV2::Integration`

AWS Config 규칙: apigatewayv2-integration-private-https-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 API Gateway V2 통합에 프라이빗 연결에 대해 HTTPS가 활성화되어 있는지 확인합니다. 프라이빗 연결에 TLS가 구성되어 있지 않으면 제어가 실패합니다.

VPC 링크는 API Gateway를 프라이빗 리소스에 연결합니다. VPC 링크는 프라이빗 연결을 생성하지만 본질적으로 데이터를 암호화하지는 않습니다. TLS를 구성하면 API Gateway를 통해 클라이언트에서 백end-to-end 암호화에 HTTPS를 사용할 수 있습니다. TLS가 없으면 민감한 API 트래픽이 프라이빗 연결에서 암호화되지 않은 상태로 흐릅니다. HTTPS 암호화는 데이터 가로채기, man-in-the-middle 공격 및 자격 증명 노출로부터 프라이빗 연결을 통해 트래픽을 보호합니다.

문제 해결

API Gateway v2 통합에서 프라이빗 연결에 대해 전송 중 암호화를 활성화하려면 Amazon API Gateway 개발자 안내서의 프라이빗 통합 업데이트를 참조하세요. 프라이빗 통합이 HTTPS 프로토콜을 사용하도록 TLS 구성을 구성합니다.

[APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.

범주: 보호 > 데이터 보호 > 전송 중 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ApiGateway::DomainName`

AWS Config 규칙: apigateway-domain-name-tls-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `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`(사용자 지정할 수 없음)

이 제어는 API Gateway 도메인 이름이 권장 보안 정책을 사용하여 전송 중인 데이터를 암호화하도록 구성되어 있는지 확인합니다. API Gateway 도메인 이름이 권장 보안 정책을 사용하도록 구성되지 않은 경우 제어가 실패합니다.

이 제어는 HTTP APIs에 연결된 사용자 지정 도메인 이름에 대한 `FAILED` 결과를 생성합니다. HTTP APIs에 대한 합법적인 사용 사례가 있는 경우 조사 결과를 숨길 수 있습니다.

보안 정책은 API Gateway가 제공하는 최소 TLS 버전과 암호 제품군의 사전 정의된 조합입니다. 클라이언트가 API 또는 사용자 맞춤형 도메인 이름에 대해 TLS 핸드셰이크를 설정할 때, 보안 정책은 API Gateway가 허용하는 TLS 버전 및 암호 제품군을 강제 적용합니다. 보안 정책은 API 및 사용자 지정 도메인 이름을 클라이언트와 서버 간의 변조 및 도청과 같은 네트워크 보안 문제로부터 보호합니다. 권장 보안 정책을 사용하면 API Gateway 도메인 이름이 클라이언트와 API 간에 전송 중인 데이터를 보호하는 최신 보안 TLS 구성을 사용할 수 있습니다.

문제 해결

API Gateway 도메인 이름에 대한 TLS 보안 정책을 업데이트하려면 Amazon API Gateway 개발자 안내서의 보안 정책을 변경하는 방법을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS AppConfig

이러한 Security Hub CSPM 제어는 AWS AppConfig서비스와 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppConfig::Application`

AWS Config 규칙: `appconfig-application-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS AppConfig애플리케이션에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 애플리케이션에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 애플리케이션에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWS AppConfig애플리케이션에 태그를 추가하려면 API 참조TagResource의 섹션을 참조하세요. AWS AppConfig

[AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppConfig::ConfigurationProfile`

AWS Config 규칙: `appconfig-configuration-profile-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS AppConfig구성 프로파일에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 구성 프로파일에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 구성 프로파일에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWS AppConfig구성 프로필에 태그를 추가하려면 API 참조TagResource의 섹션을 참조하세요. AWS AppConfig

[AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppConfig::Environment`

AWS Config 규칙: `appconfig-environment-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 AWS AppConfig환경에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredKeyTags. 환경에 태그 키가 없거나 파라미터 requiredKeyTags에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 requiredKeyTags가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 환경에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWS AppConfig환경에 태그를 추가하려면 API 참조TagResource의 섹션을 참조하세요. AWS AppConfig

[AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppConfig::ExtensionAssociation`

AWS Config 규칙: `appconfig-extension-association-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS AppConfig확장 연결에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 확장 연결에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 확장 연결에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWS AppConfig확장 연결에 태그를 추가하려면 API 참조TagResource의 섹션을 참조하세요. AWS AppConfig

## Amazon AppFlow에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon AppFlow 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppFlow::Flow`

AWS Config 규칙: `appflow-flow-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon AppFlow 흐름에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 흐름에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 흐름에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

Amazon AppFlow 흐름에 태그를 추가하려면 Amazon AppFlow 사용 설명서의 Amazon AppFlow에서 흐름 생성을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS App Runner

이러한 AWS Security Hub CSPM제어는 AWS App Runner서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppRunner::Service`

AWS Config 규칙: apprunner-service-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS App Runner서비스에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. App Runner 서비스에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 App Runner 서비스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWS App Runner서비스에 태그를 추가하는 방법에 대한 자세한 내용은 API 참조TagResource의 섹션을 참조하세요. AWS App Runner

[AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AppRunner::VpcConnector`

AWS Config 규칙: apprunner-vpc-connector-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS App RunnerVPC 커넥터에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. VPC 커넥터에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 VPC 커넥터에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWS App RunnerVPC 커넥터에 태그를 추가하는 방법에 대한 자세한 내용은 AWS App RunnerAPI 참조의 섹션을 참조TagResource하세요.

## 에 대한 Security Hub CSPM 제어AWS AppSync

이러한 Security Hub CSPM 제어는 AWS AppSync서비스와 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.

> **Important**
>
> Security Hub CSPM은 2026년 3월 9일에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그.AWS AppSyncnow provides default encryption on all current and future API caches를 참조하세요.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::AppSync::GraphQLApi`

AWS Config 규칙: appsync-cache-ct-encryption-at-rest

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS AppSyncAPI 캐시가 저장 시 암호화되는지 확인합니다. API 캐시가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 저장 데이터를 암호화하면 기밀성을 보호할 수 있으므로 권한이 없는 사용자가 데이터에 액세스할 수 있는 위험이 줄어듭니다.

문제 해결

AWS AppSyncAPI에 대한 캐싱을 활성화한 후에는 암호화 설정을 변경할 수 없습니다. 대신 캐시를 삭제하고 암호화를 활성화한 상태로 다시 생성해야 합니다. 자세한 내용은 AWS AppSync개발자 안내서의 캐시 암호화를 참조하세요.

[AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: PCI DSS v4.0.1/10.4.2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::AppSync::GraphQLApi`

AWS Config 규칙: `appsync-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `fieldLoggingLevel` | 필드 로깅 수준 | Enum | `ERROR`, `ALL`, `INFO`, `DEBUG` | `No default value` | |

이 제어는 AWS AppSyncAPI에 필드 수준 로깅이 켜져 있는지 확인합니다. 필드 리졸버 로그 수준이 없음으로 설정되면 제어가 실패합니다. 특정 로그 유형을 활성화해야 함을 나타내는 사용자 지정 파라

미터 값을 제공하지 않는 한, Security Hub CSPM은 필드 해석기 로그 수준이 ERROR 또는 인 경우 전달된 결과를 생성합니다ALL.

로깅 및 메트릭를 사용해 GraphQL 쿼리를 식별 및 최적화하고, 문제를 해결할 수 있습니다. forAWS AppSyncGraphQL 로깅을 활성화하면 API 요청 및 응답에 대한 자세한 정보를 얻고, 문제를 식별 및 대응하고, 규제 요구 사항을 준수하는 데 도움이 됩니다.

문제 해결

로깅을 켜려면 AWS AppSync개발자 안내서의 설정 및 구성을 AWS AppSync참조하세요.

[AppSync.4]AWS AppSyncGraphQL APIs 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: AWS::AppSync::GraphQLApi

AWS Config규칙: tagged-appsync-graphqlapi (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| requiredTagKeys | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS AppSyncGraphQL API에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. GraphQL API에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 GraphQL API에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

anAWS AppSyncGraphQL API에 태그를 추가하려면 API 참조TagResource의 섹션을 AWS AppSync 참조하세요.

[AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 암호 없는 인증

심각도: 높음

리소스 유형: `AWS::AppSync::GraphQLApi`

AWS Config 규칙: `appsync-authorization-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- `AllowedAuthorizationTypes: AWS_LAMBDA,AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS`(사용자 지정할 수 없음)

이 제어는 애플리케이션이 API 키를 사용하여 anAWS AppSyncGraphQL API와 상호 작용하는지 확인합니다. API 키로 anAWS AppSyncGraphQL API를 인증하면 제어가 실패합니다.

API 키는 애플리케이션에서 인증되지 않은 GraphQL 엔드포인트를 생성할 때 AWS AppSync서비스에 의해 생성되는 하드 코딩된 값입니다. 이 API 키가 손상되면 엔드포인트는 의도하지 않은 액세스에 취약합니다. 공개적으로 액세스할 수 있는 애플리케이션 또는 웹사이트를 지원하는 경우가 아니라면 인증에 API 키를 사용하지 않는 것이 좋습니다.

문제 해결

AWS AppSyncGraphQL API에 대한 권한 부여 옵션을 설정하려면 AWS AppSync개발자 안내서의 권한 부여 및 인증을 참조하세요.

[AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.

> **Important**
>
> Security Hub CSPM은 2026년 3월 9일에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그.AWS AppSyncnow provides default encryption on all current and future API caches를 참조하세요.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::AppSync::ApiCache`

AWS Config 규칙: appsync-cache-ct-encryption-in-transit

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS AppSyncAPI 캐시가 전송 중에 암호화되는지 확인합니다. API 캐시가 전송 중에 암호화되지 않으면 제어가 실패합니다.

전송 중 데이터는 클러스터의 노드 사이 또는 클러스터와 애플리케이션 사이와 같이 한 위치에서 다른 위치로 이동하는 데이터를 나타냅니다. 데이터는 인터넷 또는 프라이빗 네트워크 내에서 이동할 수 있습니다. 전송 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다.

문제 해결

AWS AppSyncAPI에 대한 캐싱을 활성화한 후에는 암호화 설정을 변경할 수 없습니다. 대신 캐시를 삭제하고 암호화를 활성화한 상태로 다시 생성해야 합니다. 자세한 내용은 AWS AppSync개발자 안내서의 캐시 암호화를 참조하세요.

## Amazon Athena에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Athena 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Athena.1] Athena 워크그룹은 저장 시 암호화되어야 합니다

> **Important**
>
> Security Hub CSPM은 2024년 4월에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그 단원을 참조하십시오.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

관련 요구 사항: 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)

심각도: 중간

리소스 유형: `AWS::Athena::WorkGroup`

AWS Config 규칙: athena-workgroup-encrypted-at-rest

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Athena 작업 그룹이 저장 시 암호화되었는지 확인합니다. Athena 워크그룹이 저장 시 암호화되지 않으면 제어가 실패합니다.

Athena에서는 팀, 애플리케이션 또는 다양한 워크로드에 대한 쿼리를 실행하기 위한 작업 그룹을 만들 수 있습니다. 각 워크그룹에는 모든 쿼리를 암호화할 수 있는 설정이 있습니다. Amazon

Simple Storage Service(Amazon S3) 관리형 키를 사용한 서버 측 암호화, AWS Key Management Service(AWS KMS) 키를 사용한 서버 측 암호화 또는 고객 관리형 KMS 키를 사용한 클라이언트 측 암호화를 사용할 수 있습니다. 저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 해당 데이터의 기밀성을 보호하여 권한 없는 사용자가 해당 데이터에 액세스할 수 있는 위험을 줄일 수 있습니다.

문제 해결

Athena 워크그룹에 대해 저장 시 암호화를 활성화하려면 Amazon Athena 사용 설명서의 워크그룹 편집을 참조하세요. 쿼리 결과 구성 섹션에서 쿼리 결과 암호화를 선택합니다.

[Athena.2] Athena 데이터 카탈로그에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Athena::DataCatalog`

AWS Config규칙: `tagged-athena-datacatalog` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon Athena 데이터 카탈로그에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 데이터 카탈로그에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 데이터 카탈로그에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Athena 데이터 카탈로그에 태그를 추가하려면 Amazon Athena 사용 설명서의Athena 리소스 태그 지정을 참조하세요.

[Athena.3] Athena 작업 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Athena::WorkGroup`

AWS Config규칙: `tagged-athena-workgroup` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | `No default value` |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon Athena 작업 그룹에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 작업 그룹에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 작업 그룹에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Athena 작업 그룹에 태그를 추가하려면 Amazon Athena 사용 설명서의 개별 작업 그룹에 태그 추가 및 삭제를 참조하세요.

[Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Athena::WorkGroup`

AWS Config 규칙: athena-workgroup-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Athena 작업 그룹에 대한 로깅이 활성화되었는지 여부를 확인합니다. 작업 그룹에 로깅이 활성화되어 있지 않으면 제어가 실패합니다.

감사 로그는 시스템 활동을 추적하고 모니터링합니다. 보안 침해를 감지하고, 사고를 조사하고, 규정을 준수하는 데 도움이 되는 이벤트 기록을 제공합니다. 또한 감사 로그는 조직의 전반적인 책임과 투명성을 향상시킵니다.

문제 해결

Athena 작업 그룹에 대한 로깅을 활성화하는 방법에 대한 자세한 내용은 Amazon Athena 사용 설명서의 Athena에서 CloudWatch 쿼리 지표 활성화를 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Backup

이러한 Security Hub CSPM 제어는 AWS Backup서비스와 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-9(8), NIST.800-53.r5 SI-12

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Backup::RecoveryPoint`

AWS Config 규칙: `backup-recovery-point-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Backup복구 시점이 저장 시 암호화되었는지 확인합니다. 복구 시점이 저장 시 암호화되지 않으면 제어가 실패합니다.

AWS Backup복구 시점은 백업 프로세스의 일부로 생성된 데이터의 특정 복사본 또는 스냅샷을 나타냅니다. 이는 데이터가 백업된 특정 시점을 나타내며 원본 데이터가 손실되거나 손상되거나 액세스할 수 없는 경우에 대비하여 복원 시점 역할을 합니다. 백업 복구 시점을 암호화하면 무단 액세스에 대한 별도의 보호 계층이 추가됩니다. 암호화는 백업 데이터의 기밀성, 무결성 및 보안을 보호하기 위한 모범 사례입니다.

문제 해결

AWS Backup복구 시점을 암호화하려면 AWS Backup개발자 안내서의 의 백업 암호화AWS Backup를 참조하세요.

[Backup.2]AWS Backup복구 지점에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::RecoveryPoint`

AWS Config규칙: `tagged-backup-recoverypoint` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Backup복구 시점에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 복구 지점에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그

키의 존재만 확인하고 복구 지점에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

백업 생성 시 소스 리소스에서 태그를 복사하려면 AWS Backup개발자 안내서의 백업에 태그 복사를 참조하세요.

상위/복합 복구 시점의 경우 생성 시 태그가 복사되지 않습니다. 상위/복합 복구 시점을 포함하여 기존 복구 시점에 태그를 추가하려면 AWS Backup개발자 안내서의 기존 복구 시점에 태그 추가 또는 제거를 참조하세요.

[Backup.3] AWS Backup볼트에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::BackupVault`

AWS Config규칙: `tagged-backup-backupvault` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Backup볼트에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 복구 지점에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 복구 지점에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS Backup볼트에 태그를 추가하려면

1. https://console.aws.amazon.com/backup AWS Backup콘솔을 엽니다.

2. 탐색 창에서 백업 볼트를 선택합니다.
3. 목록에서 백업 볼트를 선택합니다.
4. 백업 볼트 태그 섹션에서 태그 관리를 선택합니다.
5. 해당 태그의 키와 값을 입력합니다. 키 값 쌍을 추가하려면 새로운 태그 추가를 선택합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

[Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::ReportPlan`

AWS Config규칙: `tagged-backup-reportplan` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Backup보고서 계획에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 보고서 계획에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 보고 계획에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는

데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS Backup보고서 계획에 태그를 추가하려면

1. https://console.aws.amazon.com/backup AWS Backup콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 목록에서 백업 볼트를 선택합니다.
4. 백업 볼트 태그 섹션에서 태그 관리를 선택합니다.
5. 새로운 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 페어에 대해 반복합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

[Backup.5]AWS Backup백업 계획에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Backup::BackupPlan`

AWS Config규칙: `tagged-backup-backupplan` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Backup백업 계획에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 백업 계획에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 백업 계획에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS Backup백업 계획에 태그를 추가하려면

1. https://console.aws.amazon.com/backup AWS Backup콘솔을 엽니다.
2. 탐색 창에서 백업 볼트를 선택합니다.
3. 목록에서 백업 볼트를 선택합니다.

4. 백업 볼트 태그 섹션에서 태그 관리를 선택합니다.
5. 새로운 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 페어에 대해 반복합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

## 에 대한 Security Hub CSPM 제어AWS Batch

이러한 Security Hub CSPM 제어는 AWS Batch서비스와 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Batch::JobQueue`

AWS Config 규칙: batch-job-queue-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Batch작업 대기열에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 작업 대기열에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하며 작업 대기열에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

배치 작업 대기열에 태그를 추가하려면 AWS Batch 사용 설명서의 리소스에 태그 지정을 참조하세요.

[Batch.2] 배치 예약 정책에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Batch::SchedulingPolicy`

AWS Config 규칙: batch-scheduling-policy-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 AWS Batch예약 정책에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 예약 정책에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 예약 정책에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

배치 예약 정책에 태그를 추가하려면 AWS Batch 사용 설명서의 리소스에 태그 지정을 참조하세요.

[Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Batch::ComputeEnvironment`

AWS Config 규칙: batch-compute-environment-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Batch컴퓨팅 환경에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 컴퓨팅 환경에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 컴퓨팅 환경에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

배치 컴퓨팅 환경에 태그를 추가하려면 AWS Batch 사용 설명서의 리소스에 태그 지정을 참조하세요.

[Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Batch::ComputeEnvironment`

AWS Config 규칙: batch-managed-compute-env-compute-resources-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 관리형 AWS Batch 컴퓨팅 환경의 컴퓨팅 리소스 속성에 `requiredKeyTags` 파라미터에 지정된 태그 키가 있는지 확인합니다. 컴퓨팅 리소스 속성에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 컴퓨팅 리소스 속성에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다. 이 제어는 비관리형 컴퓨팅 환경 또는 AWS Fargate리소스를 사용하는 관리형 환경을 평가하지 않습니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC

권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

관리형 컴퓨팅 환경에서 AWS Batch컴퓨팅 리소스에 태그를 추가하는 방법에 대한 자세한 내용은 AWS Batch사용 설명서의 리소스 태그 지정을 참조하세요.

## Amazon Bedrock에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Bedrock 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Bedrock.1] Amazon Bedrock 데이터 소스는 고객 관리형 AWS KMS키로 암호화해야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Bedrock::DataSource`

AWS Config 규칙: bedrock-data-source-encryption-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock 데이터 소스가 고객 관리형 AWS KMS키로 저장 시 암호화되는지 확인합니다. 데이터 소스가 고객 관리형 KMS 키로 암호화되지 않으면 제어가 실패합니다.

기본적으로 Amazon Bedrock은 AWS관리형 키를 사용하여 데이터 소스 콘텐츠를 암호화합니다. 고객 관리형 KMS 키를 사용하면 교체, 액세스 정책, 감사 등 암호화 키 수명 주기를 완벽하게 제어할 수 있습니다AWS CloudTrail. 이를 통해 지식 기반에 수집된 민감한 데이터에 대해 고객 제어 암호화를 의무화하는 규정 준수 요구 사항을 충족할 수 있습니다.

문제 해결

고객 관리형 KMS 키로 Amazon Bedrock 데이터 소스를 암호화하려면 Amazon Bedrock 사용 설명서의 Amazon Bedrock 지식 기반의 데이터 소스 수정을 참조하세요.

## Amazon Bedrock AgentCore에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Bedrock AgentCore 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::BedrockAgentCore::Runtime`

AWS Config 규칙: bedrockagentcore-runtime-private-network-required

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock AgentCore 런타임이 VPC 네트워크 모드로 구성되어 있는지 확인합니다. 런타임의 네트워크 모드가 PUBLIC으로 설정된 경우 제어가 실패합니다.

Amazon Bedrock AgentCore 런타임에 퍼블릭 네트워크 모드를 사용하면 런타임이 인터넷에 직접 노출되어 공격 표면과 무단 액세스 위험이 증가합니다. VPC 네트워크 모드로 런타임을 구성하면 프라이빗 네트워크 내에서 런타임 트래픽이 제한되므로 보안 그룹, 네트워크 ACLs 및 VPC 흐름 로그와 같은 네트워크 수준 보안 제어를 적용할 수 있습니다.

문제 해결

이 결과를 해결하려면 규정을 준수하지 않는 Bedrock AgentCore 런타임을 업데이트하고 VPC 네트워크 모드로 구성합니다. 지침은 Amazon Bedrock AgentCore 개발자 안내서의 Configure Amazon Bedrock AgentCore Runtime and tools for VPC를 참조하세요.  AgentCore

[BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::BedrockAgentCore::Gateway`

AWS Config 규칙: bedrockagentcore-gateway-authorizer-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock AgentCore Gateway에 인바운드 요청에 대한 권한이 필요한지 여부를 확인합니다. Bedrock AgentCore Gateway에 인바운드 권한 부여가 설정되어 있지 않으면 제어가 실패합니다.

Amazon Bedrock AgentCore 게이트웨이에서 인증을 구성하면 권한이 있는 클라이언트만 AI 에이전트에게 요청을 보낼 수 있습니다. 권한 부여자가 없으면 게이트웨이 엔드포인트에 대한 네트워크 액세스 권한이 있는 모든 엔터티가 에이전트를 호출하여 무단 데이터 액세스, 리소스 남용 또는 예상치 못한 비용이 발생할 수 있습니다. 인바운드 권한 부여는 AgentCore 게이트웨이를 통해 대상에 액세스하려고 시도하는 사용자를 검증합니다.

문제 해결

Amazon Bedrock AgentCore Gateway에 대한 인바운드 권한 부여를 설정하려면 Amazon Bedrock AgentCore 개발자 안내서의 게이트웨이에 대한 인바운드 권한 부여 설정을 참조하세요.

[BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::BedrockAgentCore::Memory`

AWS Config 규칙: bedrock-agentcore-memory-encryption-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock AgentCore 메모리가 고객 관리형 AWS KMS키로 저장 시 암호화되는지 확인합니다. Bedrock AgentCore 메모리가 고객 관리형 KMS 키로 암호화되지 않으면 제어가 실패합니다.

Amazon Bedrock AgentCore 메모리 암호화에 고객 관리형 KMS 키를 사용하면 기본 서비스 관리형 키에 비해 보안이 향상됩니다. 고객 관리형 KMS 키를 사용하면 암호화 키 수명 주기 및 액세스 정책을 완벽하게 제어할 수 있습니다. 또한 모든 암호화 키 사용량은 감사 가능성을 AWS CloudTrail위해를 통해 로깅하고 모니터링할 수 있습니다.

문제 해결

고객 관리형 KMS 키로 Amazon Bedrock AgentCore 메모리를 암호화하려면 Amazon Bedrock AgentCore 개발자 안내서의 Amazon Bedrock AgentCore 메모리 암호화를 참조하세요.  AgentCore

[BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::BedrockAgentCore::Gateway`

AWS Config 규칙: bedrockagentcore-gateway-encryption-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock AgentCore Gateway가 고객 관리형 AWS KMS키로 저장 시 암호화되는지 확인합니다. Bedrock AgentCore Gateway가 고객 관리형 KMS 키로 암호화되지 않은 경우 제어가 실패합니다.

기본적으로 Amazon Bedrock AgentCore는 AWS관리형 키를 사용하여 게이트웨이 데이터를 암호화합니다. 고객 관리형 KMS 키를 사용하면 교체, 액세스 정책, 감사 등 암호화 키 수명 주기를 완벽하게 제어할 수 있습니다AWS CloudTrail. 이를 통해 민감한 AI 워크로드에 대한 고객 제어 암호화를 요구하는 규정 준수 요구 사항을 충족할 수 있습니다.

문제 해결

고객 관리형 KMS 키로 Bedrock AgentCore Gateway를 암호화하려면 Amazon Bedrock AgentCore 개발자 안내서의 고객 관리형 KMS 키로 AgentCore 게이트웨이 암호화를 참조하세요. AgentCore

[BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 높음

리소스 유형: `AWS::BedrockAgentCore::BrowserCustom`

AWS Config 규칙: bedrockagentcore-browsercustom-network-mode-not-public

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock AgentCore 사용자 지정 브라우저가 퍼블릭 네트워크 모드로 구성되어 있는지 확인합니다. 네트워크 모드가 퍼블릭으로 설정된 경우 제어가 실패합니다.

Amazon Bedrock AgentCore 사용자 지정 브라우저에 PUBLIC 네트워크 모드를 사용하면 브라우저 세션이 인터넷에 직접 노출되어 공격 표면과 무단 액세스 위험이 증가합니다. VPC 네트워크 모드로 브라우저를 구성하면 브라우저 트래픽이 프라이빗 네트워크 내에서 제한되므로 보안 그룹, 네트워크 ACLs 및 VPC 흐름 로그와 같은 네트워크 수준 보안 제어를 적용할 수 있습니다.

문제 해결

이 결과를 해결하려면 규정을 준수하지 않는 Bedrock AgentCore 사용자 지정 브라우저를 삭제하고 VPC 네트워크 모드로 다시 생성합니다. 지침은 Amazon Bedrock AgentCore 개발자 안내서의 Configure Amazon Bedrock AgentCore Runtime and tools for VPC를 참조하세요. AgentCore

[BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::BedrockAgentCore::BrowserCustom`

AWS Config 규칙: bedrockagentcore-browsercustom-recording-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock AgentCore 사용자 지정 브라우저에 S3 대상이 구성된 세션 레코딩이 활성화되어 있는지 확인합니다. 사용자 지정 브라우저에 레코딩이 활성화되어 있지 않거나 레코딩을 저장하도록 구성된 S3 위치가 없는 경우 제어가 실패합니다.

Bedrock AgentCore 사용자 지정 브라우저에 대한 세션 레코딩은 브라우저 상호 작용의 전체 감사 가능성을 보장하여 자동 브라우징 세션 중에 무단 액세스, 데이터 유출 또는 악의적인 활동을 탐지할 수 있습니다.

문제 해결

브라우저 세션 레코딩을 활성화하는 방법에 대한 지침은 Amazon Bedrock AgentCore 개발자 안내서의 세션 레코딩 및 재생을 참조하세요.

[BedrockAgentCore.7] Bedrock AgentCore 사용자 지정 코드 인터프리터는 프라이빗 네트워크 구성을 사용해야 합니다.

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 높음

리소스 유형: `AWS::BedrockAgentCore::CodeInterpreterCustom`

AWS Config 규칙: bedrockagentcore-codeinterpreter-networkmode-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Bedrock AgentCore 사용자 지정 코드 인터프리터가 프라이빗 네트워크 모드로 구성되어 있는지 확인합니다. 네트워크 모드가 `PUBLIC` 또는 로 설정된 경우 제어가 실패합니다`SANDBOX`.

프라이빗 네트워크 모드로 Bedrock AgentCore 사용자 지정 코드 인터프리터를 구성하면 코드 실행 환경이 VPC 내에서 격리됩니다. 퍼블릭 또는 샌드박스 네트워크 모드는 코드 인터프리터를 인터넷에 노출하여 무단 액세스 및 데이터 유출 위험을 높입니다. 프라이빗 네트워크 모드를 사용하면 네트워크 액세스를 제한하고 코드 해석 중에 처리되는 민감한 데이터를 보호할 수 있습니다.

문제 해결

이 결과를 해결하려면 규정을 준수하지 않는 Bedrock AgentCore 사용자 지정 코드 인터프리터를 삭제하고 VPC 네트워크 모드로 다시 생성합니다. 지침은 Amazon Bedrock AgentCore 개발자 안내서의 런타임 및 도구에 대한 VPC 액세스 구성을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Certificate Manager

이러한 AWS Security Hub CSPM제어는 AWS Certificate Manager(ACM) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ACM::Certificate`

AWS Config 규칙: acm-certificate-expiration-check

스케줄 유형: 변경이 트리거되며 주기적임

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `daysToExpiration` | ACM 인증서를 갱신해야 하는 기간(일수) | Integer | `14~365` | `30` |

이 제어는 지정된 기간 내에 AWS Certificate Manager(ACM) 인증서가 갱신되었는지 확인합니다. 가져온 인증서와 ACM에서 제공하는 인증서를 모두 확인합니다. 인증서가 지정된 기간 내에 갱신되지 않으면 제어가 실패합니다. 갱신 기간 동안 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 30일을 사용합니다.

ACM은 DNS 검증을 사용하는 인증서를 자동으로 갱신할 수 있습니다. 이메일 검증을 사용하는 인증서의 경우, 도메인 검증 이메일에 응답해야 합니다. ACM은 사용자가 가져오는 인증서를 자동으로 갱신하지 않습니다. 사용자는 가져온 인증서를 수동으로 갱신해야 합니다.

문제 해결

ACM은 Amazon에서 발급한 SSL/TLS 인증서에 대한 관리형 갱신을 제공합니다. 즉, ACM은 인증서를 자동으로 갱신하거나(DNS 검증을 사용하는 경우) 인증서 만료가 가까워지면 이메일 알림을 보냅니다. 이러한 서비스는 퍼블릭 및 프라이빗 ACM 인증서 모두에 대해 제공됩니다.

이메일로 검증된 도메인의 경우

인증서 만료 후 45일이 지나면 ACM은 도메인 소유자에게 각 도메인 이름에 대한 이메일을 보냅니다. 도메인을 검증하고 갱신을 완료하려면 이메일 알림에 응답해야 합니다.

자세한 내용은 AWS Certificate Manager 사용 설명서의 이메일로 검증된 도메인의 갱신을 참조하세요.

DNS로 검증된 도메인의 경우

ACM은 DNS 검증을 사용하는 인증서를 자동으로 갱신합니다. 만료 60일 전에 ACM은 인증서를 갱신할 수 있는지 확인합니다.

도메인 이름을 검증할 수 없는 경우, ACM은 수동 검증이 필요하다는 알림을 보냅니다. 만료일 45일, 30일, 7일 및 1일 전에 이러한 알림을 보냅니다.

자세한 내용은 AWS Certificate Manager 사용 설명서의 DNS로 검증된 도메인의 갱신을 참조하세요.

[ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/4.2.1

범주: 식별 > 인벤토리 > 인벤토리 서비스

심각도: 높음

리소스 유형: `AWS::ACM::Certificate`

AWS Config 규칙: acm-certificate-rsa-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는에서 관리하는 RSA 인증서가 2,048비트 이상의 키 길이를 AWS Certificate Manager사용하는지 확인합니다. 키 길이가 2,048비트보다 작으면 제어가 실패합니다.

암호화의 강도는 키 크기와 직접적인 상관관계가 있습니다. 컴퓨팅 성능이 저하되고 서버가 더 발전함에 따라 AWS리소스를 보호하려면 최소 2,048비트의 키 길이를 사용하는 것이 좋습니다.

문제 해결

ACM에서 발급한 RSA 인증서의 최소 키 길이는 이미 2,048비트입니다. ACM으로 새로운 RSA 인증서를 발급하는 방법에 대한 지침은 AWS Certificate Manager 사용 설명서의 인증서 발급 및 관리를 참조하세요.

ACM을 사용하면 키 길이가 더 짧은 인증서를 가져올 수 있지만 이 제어를 통과하려면 최소 2,048비트의 키를 사용해야 합니다. 인증서를 가져온 후에는 키 길이를 변경할 수 없습니다. 대신 키 길이가 2,048비트보다 작은 인증서를 삭제해야 합니다. 인증서를 ACM으로 가져오는 방법에 대한 자세한 내용은 AWS Certificate Manager 사용 설명서의 인증서 가져오기 사전 조건을 참조하세요.

[ACM.3] ACM 인증서에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::ACM::Certificate`

AWS Config규칙: `tagged-acm-certificate` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Certificate Manager(ACM) 인증서에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 인증서에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된

모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 인증서에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

ACM 인증서에 태그를 추가하려면 AWS Certificate Manager사용 설명서의 AWS Certificate Manager 인증서 태그 지정을 참조하세요.

## 에 대한 Security Hub CSPM 제어CloudFormation

이러한 Security Hub CSPM 제어는 AWS CloudFormation서비스와 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[클라우드포메이션.1] CloudFormation 스택은 SNS(Simple Notification Service)와 통합되어야 합니다.

> **Important**
>
> Security Hub CSPM은 2024년 4월에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그 단원을 참조하십시오.

관련 요구 사항: NIST.800-53.r5 SI-4(12), NIST.800-53.r5 SI-4(5)

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::CloudFormation::Stack`

AWS Config 규칙: `cloudformation-stack-notification-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Simple Notification Service 알림이 CloudFormation 스택과 통합되었는지 여부를 확인합니다. 연결된 SNS 알림이 없는 경우, CloudFormation 스택에 대한 제어가 실패합니다.

CloudFormation 스택으로 SNS 알림을 구성하면 스택에서 발생하는 모든 이벤트 또는 변경 사항을 이해 관계자에게 즉시 알릴 수 있습니다.

문제 해결

CloudFormation 스택과 SNS 주제를 통합하려면 AWS CloudFormation 사용 설명서의 스택 직접 업데이트를 참조하세요.

[CloudFormation.2] CloudFormation 스택에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::CloudFormation::Stack`

AWS Config규칙: `tagged-cloudformation-stack` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 AWS CloudFormation스택에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 스택에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 서비스에 스택에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

CloudFormation 스택에 태그를 추가하려면 AWS CloudFormation API 참조의 CreateStack을 참조하세요.

[CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 중간

리소스 유형: `AWS::CloudFormation::Stack`

AWS Config 규칙: cloudformation-termination-protection-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS CloudFormation스택에 종료 방지 기능이 활성화되어 있는지 확인합니다. CloudFormation 스택에서 종료 방지 기능이 활성화되지 않은 경우 제어가 실패합니다.

CloudFormation은 관련 리소스를 Stack이라는 단일 단위로 관리하는 데 도움이 됩니다. 스택의 종료 방지 기능을 활성화하여 스택이 실수로 삭제되는 것을 방지할 수 있습니다. 종료 방지 기능이 활성화된 스택을 삭제하려고 시도하면 삭제가 실패하고 스택은 상태를 포함하여 변함없이 그대로 유지됩니다. `DELETE_IN_PROGRESS` 또는 `DELETE_COMPLETE`를 제외한 모든 상태의 스택에 종료 보호를 설정할 수 있습니다.

> **Note**
>
> 스택 종료 방지 기능을 활성화하거나 비활성화하면 해당 스택에 속한 모든 중첩 스택에 대해서도 동일한 선택 사항이 전달됩니다. 종료 방지 기능을 중첩 스택에서 직접 활성화하거나 비활성화할 수 없습니다. 종료 방지 기능이 활성화된 스택에 속한 중첩 스택은 직접 삭제할 수 없습니다. 스택 이름 옆에 NESTED가 표시되면 그 스택은 중첩 스택입니다. 중첩 스택이 속한 루트 스택에서만 종료 방지 기능을 변경 할 수 있습니다.

문제 해결

CloudFormation 스택에서 종료 방지를 활성화하려면 AWS CloudFormation사용 설명서의 CloudFormation 스택이 삭제되지 않도록 보호를 참조하세요.

[CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.

범주: 감지 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::CloudFormation::Stack`

AWS Config 규칙: cloudformation-stack-service-role-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS CloudFormation스택에 연결된 서비스 역할이 있는지 확인합니다. 연결된 서비스 역할이 없는 경우 CloudFormation 스택에 대한 제어가 실패합니다.

서비스 관리형 StackSets는 AWSOrganizations의 신뢰할 수 있는 액세스 통합을 통해 실행 역할을 사용합니다. 또한이 제어는 서비스 관리형 StackSets에 의해 생성된 AWS CloudFormation스택에 대해 FAILED 결과를 생성합니다. 연결된 서비스 역할이 없기 때문입니다. 서비스 관리형 StackSets의 인증 방식으로 인해 이러한 스택에 대해 `roleARN` 필드를 채울 수 없습니다.

CloudFormation 스택과 함께 서비스 역할을 사용하면 스택을 생성/업데이트하는 사용자와 CloudFormation에서 리소스를 생성/업데이트하는 데 필요한 권한을 분리하여 최소 권한 액세스를 구현할 수 있습니다. 이렇게 하면 권한 에스컬레이션의 위험이 줄어들고 다양한 운영 역할 간의 보안 경계를 유지하는 데 도움이 됩니다.

> **Note**
>
> 스택이 생성된 후에는 스택에 연결된 서비스 역할을 제거할 수 없습니다. 이 스택에서 작업을 수행할 수 있는 권한이 있는 다른 사용자는 `iam:PassRole` 권한의 보유 여부와 상관없이 이 역할을 사용할 수 있습니다. 역할에 사용자에게 불필요한 권한이 포함되어 있는 경우 사용자의 권한을 실수로 에스컬레이션할 수 있습니다. 이 역할은 최소 권한을 부여해야 합니다.

문제 해결

서비스 역할을 CloudFormation 스택과 연결하려면 AWS CloudFormation사용 설명서의 CloudFormation 서비스 역할을 참조하세요.

## Amazon CloudFront에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon CloudFront 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SC-7(11), NIST.800-53.r5 SC-7(16), PCI DSS v4.0.1/2.2.6

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-default-root-object-configured

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 S3 오리진을 사용하는 Amazon CloudFront 배포가 기본 루트 객체인 특정 객체를 반환하도록 구성되어 있는지 여부를 확인합니다. CloudFront 배포가 S3 오리진을 사용하고 기본 루트 객체가 구성되어 있지 않은 경우 제어가 실패합니다. 이 제어는 사용자 지정 오리진을 사용하는 CloudFront 배포에는 적용되지 않습니다.

사용자가 배포의 객체 대신 배포의 루트 URL을 요청하는 경우가 있습니다. 이 경우, 기본 루트 객체를 지정하면 웹 배포 내용이 노출되는 것을 방지하는 데 도움이 될 수 있습니다.

문제 해결

CloudFront 배포의 기본 루트 객체를 구성하려면 Amazon CloudFront 개발자 안내서의 기본 루트 객체를 지정하는 방법을 참조하세요.

[CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-viewer-policy-https

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon CloudFront 배포에서 최종 사용자가 HTTPS를 직접 사용하도록 요구하는지 또는 리디렉션을 사용하는지 여부를 확인합니다. `ViewerProtocolPolicy`가

`defaultCacheBehavior`용 또는 `cacheBehaviors`용으로 `allow-all`로 설정된 경우, 제어가 실패합니다.

HTTPS(TLS)를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 사용하여 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다.

문제 해결

전송 중인 CloudFront 배포를 암호화하려면 Amazon CloudFront 개발자 안내서의 최종 사용자와 CloudFront 간의 통신에 HTTPS 요청을 참조하세요.

[CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 낮음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-origin-failover-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon CloudFront 배포가 오리진이 두 개 이상 있는 오리진 그룹으로 구성되어 있는지 여부를 확인합니다.

CloudFront 오리진 장애 조치는 가용성을 높일 수 있습니다. 오리진 장애 조치는 기본 오리진을 사용할 수 없거나 특정 HTTP 응답 상태 코드를 반환하는 경우, 트래픽을 보조 오리진으로 자동 리디렉션합니다.

문제 해결

CloudFront 배포를 위한 오리진 장애 조치를 구성하려면 Amazon CloudFront 개발자 안내서의 오리진 그룹 생성을 참조하세요.

[CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-accesslogs-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 CloudFront 배포에서 서버 액세스 로깅이 활성화되어 있는지 여부를 확인합니다. 배포에 대한 액세스 로깅이 활성화되지 않은 경우, 제어가 실패합니다. 이 제어는 배포에 표준 로깅(레거시)이 활성화되어 있는지 여부만 평가합니다.

CloudFront 액세스 로그는 CloudFront가 수신하는 모든 사용자 요청에 대한 세부 정보를 제공합니다. 각 로그에는 요청이 수신된 날짜 및 시간, 요청한 뷰어의 IP 주소, 요청 소스, 뷰어의 요청 포트 번호 등의 정보가 포함됩니다. 이러한 로그는 보안 및 액세스 감사, 포렌식 조사와 같은 목적에 유용합니다. 액세스 로그 분석에 대한 자세한 내용은 Amazon Athena 사용 설명서의 Amazon CloudFront 로그 쿼리를 참조하세요.

문제 해결

CloudFront 배포에 대한 표준 로깅(레거시)을 구성하려면 Amazon CloudFront 개발자 안내서의 표준 로깅(레거시) 구성을 참조하세요.

[CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), PCI DSS v4.0.1/6.4.2

범주: 보호 > 보호 서비스

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-associated-with-waf

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 CloudFront 배포가 Classic 또는 AWS WAF 웹 ACLs과 AWS WAF 연결되어 있는지 확인합니다. 배포가 웹 ACL과 연결되어 있지 않으면 제어가 실패합니다.

AWS WAF 는 웹 애플리케이션 및 APIs으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 사용자가 정의한 맞춤형 웹 보안 규칙 및 조건에 따라 웹 요청을 허용, 차단 또는 계산하는 규칙 집합(웹 액세스 제어 목록 또는 웹 ACL)을 구성할 수 있습니다. CloudFront 배포가 AWS WAF 웹 ACL과 연결되어 있는지 확인하여 악의적인 공격으로부터 보호합니다.

문제 해결

AWS WAF 웹 ACL을 CloudFront 배포와 연결하려면 Amazon CloudFront 개발자 안내서의 AWS WAF를 사용하여 콘텐츠에 대한 액세스 제어를 참조하세요.

[CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 낮음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-custom-ssl-certificate

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 CloudFront 배포가 CloudFront에서 제공하는 기본 SSL/TLS 인증서를 사용하고 있는지 여부를 확인합니다. CloudFront 배포에서 사용자 지정 SSL/TLS 인증서를 사용하는 경우, 이 제어가 통과됩니다. CloudFront 배포에서 기본 SSL/TLS 인증서를 사용하는 경우, 이 제어가 실패합니다.

사용자 지정 SSL/TLS를 사용하면 사용자가 대체 도메인 이름을 사용하여 콘텐츠에 액세스할 수 있습니다. 사용자 지정 인증서를 AWS Certificate Manager (권장) 또는 IAM에 저장할 수 있습니다.

문제 해결

사용자 지정 SSL/TLS 인증서를 사용하여 CloudFront 배포에 대체 도메인 이름을 추가하려면 Amazon CloudFront 개발자 안내서의 대체 도메인 이름 추가를 참조하세요.

[CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-sni-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon CloudFront 배포가 사용자 지정 SSL/TLS 인증서를 사용하고 있고 SNI를 사용하여 HTTPS 요청을 처리하도록 구성되어 있는지 확인합니다. 사용자 지정 SSL/TLS 인증서가 연결되어 있지만 SSL/TLS 지원 방법이 전용 IP 주소인 경우, 이 제어는 실패합니다. 배포에서 기본 CloudFront SSL/TLS 인증서를 사용하는 경우에도 제어가 실패합니다.

서버 이름 표시(SNI)는 2010년 이후 출시된 브라우저와 클라이언트에서 지원되는 TLS 프로토콜의 확장 기능입니다. SNI를 사용하여 HTTPS 요청을 제공하도록 CloudFront를 구성한 경우, CloudFront에서는 대체 도메인 이름을 각 엣지 로케이션의 IP 주소와 연결합니다. 최종 사용자가 HTTPS 콘텐츠 요청을 제출하면 DNS는 이 요청을 올바른 엣지 로케이션의 IP 주소로 라우팅합니다. 도메인 이름의 IP 주소는 SSL/TLS 핸드셰이크 협상 중에 결정됩니다(IP 주소는 배포 전용이 아님).

문제 해결

SNI를 사용하여 HTTPS 요청을 처리하도록 CloudFront 배포를 구성하려면 CloudFront 개발자 안내서의 SNI를 사용하여 HTTPS 요청 제공(대부분의 클라이언트에서 작동)을 참조하세요. 사용자 지정 SSL 인증서에 대한 자세한 내용은 CloudFront에서 SSL/TLS 인증서를 사용하기 위한 요구 사항을 참조하세요.

[CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-traffic-to-origin-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon CloudFront 배포가 사용자 지정 오리진에 대한 트래픽을 암호화하고 있는지 확인합니다. 오리진 프로토콜 정책이 'http-only'를 허용하는 CloudFront 배포에서는 이 제어가 실패합니다. 배포의 원본 프로토콜 정책이 'match-viewer'이고 뷰어 프로토콜 정책이 'all-all'인 경우에도 이 제어가 실패합니다.

HTTPS(TLS)를 사용하면 네트워크 트래픽의 도청이나 조작을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다.

문제 해결

CloudFront 연결에 암호화를 요구하도록 오리진 프로토콜 정책을 업데이트하려면 Amazon CloudFront 개발자 안내서의 CloudFront와 사용자 지정 오리진 간 통신에 HTTPS 요청을 참조하세요.

[CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

관련 요구 사항: 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), NIST.800-53.r5 SC-8(2), NIST.800-53.r5 SI-7(6), NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-no-deprecated-ssl-protocols

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon CloudFront 배포가 CloudFront 엣지 로케이션과 사용자 지정 오리진 간의 HTTPS 통신에 더 이상 사용되지 않는 SSL 프로토콜을 사용하고 있는지 확인합니다. CloudFront 배포에 `CustomOriginConfig`가 있고 `OriginSslProtocols`가 `SSLv3`를 포함하는 경우, 이 제어가 실패합니다.

2015년 IETF(Internet Engineering Task Force)는 SSL 3.0의 보안이 충분하지 않기 때문에 더 이상 사용되지 않아야 한다고 공식적으로 발표했습니다. 사용자 지정 오리진에 대한 HTTPS 통신에는 TLSv1.2 이상을 사용하는 것이 좋습니다.

문제 해결

CloudFront 배포를 위한 오리진 SSL 프로토콜을 업데이트하려면 Amazon CloudFront 개발자 안내서의 CloudFront와 사용자 지정 오리진 간의 통신을 위한 HTTPS 요청을 참조하세요.

[CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2), PCI DSS v4.0.1/2.2.6

범주: 식별 > 리소스 구성

심각도: 높음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-s3-origin-non-existent-bucket

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon CloudFront 배포가 존재하지 않는 Amazon S3 오리진을 가리키는지 여부를 확인합니다. 오리진이 존재하지 않는 버킷을 가리키도록 구성된 경우, CloudFront 배포에 대한 제어가 실패합니다. 이 제어는 정적 웹 사이트 호스팅이 없는 S3 버킷이 S3 오리진인 CloudFront 배포에만 적용됩니다.

계정의 CloudFront 배포가 존재하지 않는 버킷을 가리키도록 구성된 경우, 악의적인 제3자가 참조된 버킷을 생성하고 배포를 통해 자체 콘텐츠를 제공할 수 있습니다. 라우팅 동작에 관계없이 모든 오리진을 검사하여 배포가 적절한 오리진을 가리키고 있는지 확인하는 것이 좋습니다.

문제 해결

새로운 오리진을 가리키도록 CloudFront 배포를 수정하려면 Amazon CloudFront 개발자 안내서의 배포 업데이트를 참조하세요.

[CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-s3-origin-access-control-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 오리진과 함께 Amazon CloudFront 배포에 오리진 액세스 제어(OAC)가 구성되어 있는지 확인합니다. CloudFront 배포에 대해 OAC가 구성되지 않은 경우, 제어가 실패합니다.

S3 버킷을 CloudFront 배포의 오리진으로 사용하는 경우, OAC를 활성화할 수 있습니다. 이렇게 하면 지정된 CloudFront 배포를 통해서만 버킷의 콘텐츠에 액세스할 수 있고, 버킷이나 다른 배포에서 직접 액세스하는 것은 금지합니다. CloudFront는 오리진 액세스 ID(OAI)를 지원하지만 OAC는 추가 기능을 제공하며 OAI를 사용하는 배포는 OAC로 마이그레이션할 수 있습니다. OAI는 S3 오리진에 액세스하는 안전한 방법을 제공하지만 세분화된 정책 구성 및 AWS 서명 버전 4(SigV4)가 필요한에서 POST 메서드를 사용하는 HTTP/HTTPS 요청에 대한 지원 부족과 같은 제한 사항이 AWS 리전 있습니다. 또한 OAI는를 사용한 암호화를 지원하지 않습니다 AWS Key Management Service. OAC는 IAM 서비스 보안 주체를 사용하여 S3 오리진으로 인증하는 AWS 모범 사례를 기반으로 합니다.

문제 해결

S3 오리진을 사용하여 CloudFront 배포에 대해 OAC를 구성하려면 Amazon CloudFront 개발자 안내서의 Amazon S3 오리진에 대한 액세스 제한을 참조하세요.

[CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙:`tagged-cloudfront-distribution` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon CloudFront 배포에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 배포에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 서비스에 배포에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

CloudFront 배포에 태그를 추가하려면 Amazon CloudFront 개발자 안내서의 Amazon CloudFront 배포 태그 지정을 참조하세요.

[CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-ssl-policy-check

스케줄 유형: 변경이 트리거됨

파라미터: `securityPolicies`: `TLSv1.2_2021,TLSv1.2_2025,TLSv1.3_2025`(사용자 지정할 수 없음)

이 제어는 Amazon CloudFront 배포가 권장 TLS 보안 정책을 사용하도록 구성되어 있는지 확인합니다. CloudFront 배포가 권장 TLS 보안 정책을 사용하도록 구성되지 않은 경우 제어가 실패합니다.

최종 사용자가 HTTPS를 사용하여 콘텐츠에 액세스하도록 Amazon CloudFront 배포를 구성하는 경우, 보안 정책을 선택하고 사용할 최소 SSL/TLS 프로토콜 버전을 지정해야 합니다. 이는 CloudFront가 최종 사용자와 통신하는 데 사용하는 프로토콜 버전과 CloudFront가 통신을 암호화하는 데 사용하는 암호를 결정합니다. CloudFront에서 제공하는 최신 보안 정책을 사용하는 것이 좋습니다. 이렇게 하면 CloudFront가 최신 암호 제품군을 사용하여 최종 사용자와 CloudFront 배포 간에 전송 중 데이터를 암호화할 수 있습니다.

> **Note**
>
> 이 제어는 사용자 지정 SSL 인증서를 사용하도록 구성되고 레거시 클라이언트를 지원하도록 구성되지 않은 CloudFront 배포에 대해서만 조사 결과를 생성합니다.

문제 해결

CloudFront 배포의 보안 정책을 구성하는 방법에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 배포 업데이트를 참조하세요. 배포의 보안 정책을 구성할 때 최신 보안 정책을 선택합니다.

[CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-origin-lambda-url-oac-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Lambda 함수 URL이 오리진인 Amazon CloudFront 배포에 오리진 액세스 제어(OAC)가 활성화되어 있는지 확인합니다. CloudFront 배포가 Lambda 함수 URL을 오리진으로 사용하고 OAC가 활성화되지 않은 경우 제어가 실패합니다.

AWS Lambda 함수 URL은 Lambda 함수의 전용 HTTPS 엔드포인트입니다. Lambda 함수 URL이 CloudFront 배포의 오리진인 경우 함수 URL에 공개적으로 액세스할 수 있어야 합니다. 따라서 보안 모범 사례로 OAC를 생성하고 배포의 Lambda 함수 URL에 추가해야 합니다. OAC는 IAM 서비스 위탁자를 사용하여 CloudFront와 함수 URL 간의 요청을 인증합니다. 또한 요청이 정책에 지정된 CloudFront 배포를 대신하는 경우에만 함수 간접 호출을 허용하는 리소스 기반 정책을 사용하도록 지원합니다.

문제 해결

Lambda 함수 URL을 오리진으로 사용하는 Amazon CloudFront 배포에 대해 OAC를 구성하는 방법에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 AWS Lambda 함수 URL 오리진에 대한 액세스 제한을 참조하세요.

[CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::CloudFront::Distribution`

AWS Config 규칙: cloudfront-distribution-key-group-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon CloudFront 배포가 서명된 URL 또는 서명된 쿠키 인증에 신뢰할 수 있는 키 그룹을 사용하도록 구성되어 있는지 확인합니다. CloudFront 배포에서 신뢰할 수 있는 서명자를 사용하거나 배포에 인증이 구성되지 않은 경우 제어가 실패합니다.

서명된 URL 또는 서명된 쿠키를 사용하려면 서명자가 필요합니다. 서명자는 CloudFront에서 생성하는 신뢰할 수 있는 키 그룹이거나 CloudFront 키 페어가 포함된 AWS 계정입니다. CloudFront 키 그룹에서는 AWS 계정 루트 사용자를 사용하여 CloudFront 서명된 URLs 및 서명된 쿠키의 퍼블릭 키를 관리할 필요가 없으므로 신뢰할 수 있는 키 그룹을 사용하는 것이 좋습니다.

> **Note**
>
> 이 제어는 다중 테넌트 CloudFront 배포를 평가하지 않습니다(`connectionMode=tenant-only`).

문제 해결

서명된 URLs 및 쿠키와 함께 신뢰할 수 있는 키 그룹을 사용하는 방법에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 신뢰할 수 있는 키 그룹 사용을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS CloudTrail

이러한 AWS Security Hub CSPM제어는 AWS CloudTrail서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/3.1, CIS AWS파운데이션 벤치마크 v1.2.0/2.1, CIS AWS파운데이션 벤치마크 v1.4.0/3.1, CIS AWS파운데이션 벤치마크 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.800AU-3.r5 AU-6 AU-14 CA-7 NIST.800-53.r5 SC-7 SI-3 SI-4 SI-7 SA-8

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: multi-region-cloudtrail-enabled

스케줄 유형: 주기적

파라미터:

- `readWriteType`: `ALL`(사용자 지정할 수 없음)

  `includeManagementEvents`: `true`(사용자 지정할 수 없음)

이 제어는 읽기 및 쓰기 관리 이벤트를 캡처하는 다중 리전 AWS CloudTrail추적이 하나 이상 있는지 확인합니다. CloudTrail이 비활성화되거나 읽기 및 쓰기 관리 이벤트를 캡처하는 CloudTrail 추적이 하나 이상 없는 경우, 제어가 실패합니다.

AWS CloudTrail는 계정에 대한 AWSAPI 호출을 기록하고 로그 파일을 전달합니다. 기록된 정보에는 다음 정보가 포함됩니다.

- API 호출자의 ID
- API 호출 시간
- API 호출자의 소스 IP 주소
- 요청 파라미터
- 에서 반환한 응답 요소AWS 서비스

CloudTrail은,AWS Management ConsoleAWSSDKs, 명령줄 도구에서 수행된 AWSAPI 호출을 포함하여 계정에 대한 API 호출 기록을 제공합니다. 기록에는 AWS 서비스와 같은 상위 수준의 API 호출도 포함됩니다AWS CloudFormation.

CloudTrail에서 생성한 AWSAPI 호출 기록을 통해 보안 분석, 리소스 변경 추적 및 규정 준수 감사를 수행할 수 있습니다. 다중 리전 추적에는 다음과 같은 이점이 있습니다.

- 다중 리전 추적을 통해 사용하지 않는 리전에서 발생하는 예기치 않은 활동을 감지할 수 있습니다.
- 다중 리전 추적으로 인해 기본적으로 추적에 글로벌 서비스 이벤트 로깅이 사용되도록 설정됩니다. 글로벌 서비스 이벤트 로깅은 AWS글로벌 서비스에서 생성된 이벤트를 기록합니다.
- 다중 리전 추적의 경우, 모든 읽기 및 쓰기 작업에 대한 관리 이벤트는 CloudTrail이 AWS 계정의 모든 리소스에 대한 관리 작업을 기록하도록 보장합니다.

기본적으로를 사용하여 생성된 CloudTrail 추적은 다중 리전 추적AWS Management Console입니다.

문제 해결

CloudTrail에서 새로운 다중 리전 추적을 생성하려면 AWS CloudTrail 사용 안내서의 추적 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 추가 설정, 로그 파일 검증 | 활성화됨 |
| 로그 이벤트, 관리 이벤트, API 활동 선택 | 읽기 및 쓰기. 제외 확인란을 선택 취소합니다. |

기존 추적을 업데이트하려면 AWS CloudTrail 사용 안내서의 추적 업데이트를 참조하세요. 관리 이벤트에서 API 활동의 경우, 읽기 및 쓰기를 선택합니다.

[CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/3.5, CIS AWS파운데이션 벤치마크 v1.2.0/2.7, CIS AWS파운데이션 벤치마크 v1.4.0/3.7, CIS AWS파운데이션 벤치마크 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, NIST.800-53.r5 SC-28(1), NIST.800-53.r5 SC-28( NIST.800-53.r5 SC-7 SI-710.3.21

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config 규칙: cloud-trail-encryption-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 CloudTrail이 서버 측 암호화(SSE) AWS KMS key 암호화를 사용하도록 구성되어 있는지 확인합니다. `KmsKeyId`가 정의되지 않은 경우, 제어가 실패합니다.

민감한 CloudTrail 로그 파일에 대한 보안 계층을 추가하려면 저장 시 암호화를 위해 CloudTrail 로그 파일에 AWS KMS keys(SSE-KMS)를 사용한 서버 측 암호화를 사용해야 합니다. CloudTrail 기본적으로 CloudTrail이 버킷에 제공하는 로그 파일은 Amazon S3 관리형 암호화 키(SSE-S3)를 사용하는 Amazon 서버 측 암호화로 암호화됩니다.

문제 해결

CloudTrail 로그 파일에 SSE-KMS 암호화를 활성화하려면 AWS CloudTrail 사용 설명서의 KMS 키를 사용하도록 추적 업데이트를 참조하세요.

[CloudTrail.3] 하나 이상의 CloudTrail 추적을 활성화해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: cloudtrail-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는에서 AWS CloudTrail추적이 활성화되어 있는지 확인합니다AWS 계정. 계정에 CloudTrail 추적 하나 이상 없는 경우, 제어가 실패합니다.

그러나 일부 AWS서비스는 모든 APIs 활성화하지 않습니다. CloudTrail 이외의 추가 감사 추적을 구현하고 CloudTrail 지원 서비스 및 통합의 각 서비스에 대한 설명서를 검토해야 합니다.

문제 해결

CloudTrail을 시작하고 추적을 생성하려면 AWS CloudTrail사용 설명서의 시작하기 AWS CloudTrail자습서를 참조하세요.

[CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다.

관련 요구 사항: CIS AWSFoundations Benchmark v5.0.0/3.2, CIS AWSFoundations Benchmark v1.2.0/2.2, CIS AWSFoundations Benchmark v1.4.0/3.2, CIS AWSFoundations Benchmark v3.0.0/3.2, NIST.800-53.r5 AU-9, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7(1), NIST.800-53.r5 SI-7(3), NIST.800-53.r5 SI-7(7), NIST.800-171.r2 3.8 PCIS v3.2.10.5.210.5.510.3.2

범주: 데이터 보호 > 데이터 무결성

심각도: 낮음

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config 규칙: cloud-trail-log-file-validation-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 CloudTrail 추적에서 로그 파일 무결성 검증이 활성화되어 있는지 확인합니다.

CloudTrail 로그 파일 검증은 CloudTrail이 Amazon S3에 쓰는 각 로그의 해시를 포함하는 디지털 서명 다이제스트 파일을 생성합니다. 이러한 다이제스트 파일을 사용하면 CloudTrail이 로그를 전달한 후 로그 파일이 변경, 삭제 또는 변경되지 않았는지 확인할 수 있습니다.

Security Hub CSPM은 모든 추적에서 파일 검증을 활성화할 것을 권장합니다. 로그 파일 검증은 CloudTrail 로그의 추가 무결성 검사를 제공합니다.

문제 해결

CloudTrail 로그 파일 검증을 활성화하려면 AWS CloudTrail 사용 설명서의 CloudTrail에 대한 로그 파일 무결성 검증 활성화를 참조하세요.

[CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/3.4, PCI DSS v3.2.1/10.5.3, CIS AWS파운데이션 벤치마크 v1.2.0/2.4, CIS AWS파운데이션 벤치마크 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.800-5AU-3r5 AU-2, NIST. AU-6 AU-7 CA-7 NIST.800-53.r5 SC-7 SI-20 SI-3 SI-4 SI-7

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config 규칙: cloud-trail-cloud-watch-logs-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 CloudTrail 추적이 CloudWatch Logs로 로그를 전송하도록 구성되어 있는지 확인합니다. 추적의 `CloudWatchLogsLogGroupArn` 속성이 비어 있으면 제어가 실패합니다.

CloudTrail은 지정된 계정에서 수행된 AWSAPI 호출을 기록합니다. 기록된 정보에는 다음이 포함됩니다.

- API 호출자의 ID
- API 호출 시간
- API 호출자의 소스 IP 주소
- 요청 파라미터
- 에서 반환하는 응답 요소AWS 서비스

CloudTrail은 로그 파일 저장 및 전송에 Amazon S3를 사용합니다. 장기 분석을 위해 지정된 S3 버킷에서 CloudTrail 로그를 캡처할 수 있습니다. 실시간 분석을 수행하려면 CloudTrail을 구성하여 CloudWatch Logs로 로그를 보내면 됩니다.

계정의 모든 리전에서 활성화된 추적의 경우, CloudTrail은 해당 모든 리전의 로그 파일을 CloudWatch Logs 로그 그룹으로 보냅니다.

Security Hub CSPM은 CloudTrail 로그를 CloudWatch Logs로 전송하는 것을 권장합니다. 참고로 이 권장 사항은 계정 활동을 캡처, 모니터링하고, 적절하게 경보를 받을 수 있도록 하기 위한 것입니다. CloudWatch Logs를 사용하여에서 이를 설정할 수 있습니다AWS 서비스. 이 권장 사항은 다른 솔루션의 사용을 배제하지 않습니다.

CloudTrail 로그를 CloudWatch Logs로 전송하면 사용자, API, 리소스 및 IP 주소에 근거한 실시간 및 과거 활동 로깅이 더 용이해집니다. 이 접근 방식을 사용하여 비정상적이거나 민감한 계정 활동에 대한 경보 및 알림을 설정할 수 있습니다.

문제 해결

CloudTrail을 CloudWatch Logs와 통합하려면 AWS CloudTrail 사용 설명서의 CloudWatch Logs에 이벤트 전송을 참조하세요.

[CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v1.2.0/2.3, CIS AWS파운데이션 벤치마크 v1.4.0/3.3, PCI DSS v4.0.1/1.4.4

범주: 식별 > 로깅

심각도: 심각

리소스 유형: `AWS::S3::Bucket`

AWS Config규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적이며 변경이 트리거됨

파라미터: 없음

CloudTrail은 계정에서 이루어진 모든 API 호출 기록을 기록합니다. 이 로그 파일은 S3 버킷에 저장됩니다. CIS에서는 CloudTrail이 기록하는 S3 버킷에 S3 버킷 정책 또는 ACL(액세스 제어 목록)을 적용하여 CloudTrail 로그에 대한 공개 액세스를 방지할 것을 권장합니다. CloudTrail 로그 콘텐츠에 대한 공개 액세스를 허용하면 공격자가 영향을 받는 계정의 사용 또는 구성의 약점을 식별하는 데 도움이 될 수 있습니다.

이 점검을 실행하기 위해 Security Hub CSPM은 먼저 사용자 지정 로직을 사용하여 CloudTrail 로그가 저장되는 S3 버킷을 찾습니다. 그런 다음 AWS Config관리형 규칙을 사용하여 버킷에 공개적으로 액세스할 수 있는지 확인합니다.

로그를 단일 중앙 집중식 S3 버킷으로 집계하면 Security Hub CSPM은 중앙 집중식 S3 버킷이 위치한 계정 및 리전에 대해서만 검사를 실행합니다. 기타 계정 및 리전의 경우, 제어 상태는 데이터 없음입니다.

버킷에 공개적으로 액세스할 수 있는 경우, 검사는 실패한 조사 결과를 생성합니다.

문제 해결

CloudTrail S3 버킷에 대한 퍼블릭 액세스를 차단하려면 Amazon Simple Storage Service 사용 설명서의 S3 버킷에 대한 퍼블릭 액세스 차단 설정 구성을 참조하세요. 4가지 Amazon S3 Block Public Access 설정을 모두 선택합니다.

[CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v1.2.0/2.6, CIS AWS파운데이션 벤치마크 v1.4.0/3.6, CIS AWS파운데이션 벤치마크 v3.0.0/3.4, PCI DSS v4.0.1/10.2.1

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

S3 버킷 액세스 로깅은 S3 버킷에 대한 각 요청에 대한 액세스 기록이 포함된 로그를 생성합니다. 액세스 로그 레코드에는 요청 유형, 요청과 관련된 리소스, 요청 처리 날짜/시간과 같은 요청 세부 정보가 포함됩니다.

CIS에서는 CloudTrail S3 버킷에서 버킷 액세스 로깅을 사용하도록 설정하는 것이 좋습니다.

대상 S3 버킷에서 S3 버킷 로깅을 활성화하면 대상 버킷의 객체에 영향을 미칠 수 있는 모든 이벤트를 캡처할 수 있습니다. 별도 버킷에 배치할 로그를 구성하면 로그 정보에 대한 액세스가 활성화되어 보안 및 인시던트 대응 워크플로에 유용할 수 있습니다.

이 검사를 실행하기 위해 Security Hub CSPM은 먼저 사용자 지정 로직을 사용하여 CloudTrail 로그가 저장되는 버킷을 찾은 다음 AWS Config관리형 규칙을 사용하여 로깅이 활성화되어 있는지 확인합니다.

CloudTrail이 여러의 로그 파일을 단일 대상 Amazon S3 버킷AWS 계정으로 전송하는 경우 Security Hub CSPM은 해당 버킷이 위치한 리전의 대상 버킷에 대해서만이 제어를 평가합니다. 이렇게 하면 조사 결과가 간소화됩니다. 하지만 대상 버킷에 로그를 전송하는 모든 계정에서 CloudTrail을 켜야 합니다. 대상 버킷을 보유한 계정을 제외한 모든 계정의 제어 상태는 데이터 없음입니다.

문제 해결

CloudTrail S3 버킷에 대한 서버 액세스 로깅을 활성화하려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.

[CloudTrail.9] CloudTrail 추적에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::CloudTrail::Trail`

AWS Config규칙: `tagged-cloudtrail-trail` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS CloudTrail추적에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 추적에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 서비스에 추적에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

CloudTrail 추적에 태그를 추가하려면 AWS CloudTrail API 참조의 태그 추가를 참조하세요.

[CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::CloudTrail::EventDataStore`

AWS Config 규칙: event-data-store-cmk-encryption-enabled

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `kmsKeyArns` | 평가에 AWS KMS keys포함할 의 Amazon 리소스 이름(ARNs) 목록입니다. 이벤트 데이터 저장소가 목록의 KMS 키로 암호화되지 않은 경우, 제어는 `FAILED` 조사 결과를 생성합니다. | StringList(최대 3개 항목) | 기존 KMS 키의 ARN 1~3개. 예를 들어 `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` 입니다. | 기본값 없음 |

이 제어는 AWS CloudTrailLake 이벤트 데이터 스토어가 고객 관리형으로 저장 시 암호화되는지 확인합니다AWS KMS key. 이벤트 데이터 저장소가 고객 관리형 KMS 키로 암호화되지 않은 경우 제어가 실패합니다. 선택적으로 평가에 포함할 제어에 대한 KMS 키 목록을 지정할 수 있습니다.

기본적으로 AWS CloudTrailLake는 AES-256 알고리즘을 사용하여 Amazon S3 관리형 키(SSE-S3)를 사용하여 이벤트 데이터 스토어를 암호화합니다. 추가 제어를 위해 대신 고객 관리형AWS KMS key(SSE-KMS)으로 이벤트 데이터 스토어를 암호화하도록 CloudTrail Lake를 구성할 수 있습니다. 고객 관리형 KMS 키는 AWS KMS key에서 생성, 소유 및 관리하는 입니다AWS 계정. 이러한 유형의 KMS 키는 사용자가 완전히 제어할 수 있습니다. 여기에는 키 정책 정의 및 유지 관리, 권한 부여 관리, 암호화 자료 교체, 태그 할당, 별칭 생성, 키 활성화 및 비활성화가 포함됩니다. CloudTrail 데이터에 대한 암호화 작업에서 고객 관리형 KMS 키를 사용하고 CloudTrail 로그를 통해 사용을 감사할 수 있습니다.

문제 해결

AWS KMS key지정한를 사용하여 AWS CloudTrailLake 이벤트 데이터 스토어를 암호화하는 방법에 대한 자세한 내용은 AWS CloudTrail사용 설명서의 이벤트 데이터 스토어 업데이트를 참조하세요. KMS 키와 이벤트 데이터 스토어를 연결한 후에는 KMS 키를 제거하거나 변경할 수 없습니다.

## Amazon CloudWatch에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon CloudWatch 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/1.1,CIS AWS 파운데이션 벤치마크 v1.2.0/3.3, CIS AWS 파운데이션 벤치마크 v1.4.0/1.7,CIS AWS 파운데이션 벤치마크 v1.4.0/4.3, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7, PCI DSS v3.2.1/7.2.1

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

루트 사용자에게는 AWS 계정의 모든 서비스 및 리소스에 제한 없이 액세스할 수 있습니다. 일상적인 작업에는 루트 사용자를 사용하지 않는 것이 좋습니다. 루트 사용자의 사용을 최소화하고 액세스 관리

를 위해 최소 권한 원칙을 채택하면 권한이 높은 자격 증명의 의도하지 않은 변경 및 노출 위험이 줄어듭니다.

계정 및 서비스 관리 작업 수행에 필요한 경우에만 루트 사용자 보안 인증 정보를 사용하는 것이 가장 좋습니다. AWS Identity and Access Management (IAM) 정책을 사용자가 아닌 그룹 및 역할에 직접 적용합니다. 일상적 사용을 위해 관리자를 설정하는 방법에 대한 자습서는 IAM 사용자 설명서의 첫 IAM 관리자 및 그룹 생성을 참조하세요

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.4.0에서 제어 1.7에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.
>
>   가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 결과를 생성합니다.

### 문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |
| 기본값 | **`0`** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.2] 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS Foundations Benchmark v1.2.0/3.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다.

CIS에서는 지표 필터를 생성하고 승인되지 않은 API 직접 호출에 대한 경보를 생성할 것을 권장합니다. 무단 API 호출을 모니터링하면 애플리케이션 오류를 표시하는 데 도움이 되고 악의적인 활동을 탐지하는 시간을 단축할 수 있습니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.2의 컨트롤 3.1에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

**Note**

Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 결과를 생성합니다.

### 문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.errorCode="*UnauthorizedOperation") \|\| ($.errorCode="AccessDenied*")}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |
| 기본값 | **`0`** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *`your-metric-name`* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **`1`** |

[CloudWatch.3] MFA 없는 로그인에 대해 관리 콘솔에 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.2

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다.

CIS에서는 MFA로 보호되지 않는 메트릭 필터 및 경보 콘솔 로그인을 생성할 것을 권장합니다. 단일 팩터 콘솔 로그인을 모니터링하면 MFA로 보호되지 않는 계정에 대한 가시성이 높아집니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.2의 컨트롤 3.2에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{ ($.eventName = "ConsoleLogin") && ($.additionalEventData.MFAUsed != "Yes") && ($.userIdentity.type = "IAMUser") && ($.responseElements.ConsoleLogin = "Success") }` |
| 메트릭 네임스페이스 | **LogMetrics** |
| 메트릭 값 | **1** |
| 기본값 | **0** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.4, CIS AWS 파운데이션 벤치마크 v1.4.0/4.4, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

이 제어는 CloudTrail 로그를 CloudWatch Logs로 보내고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링하는지 여부를 확인합니다.

CIS에서는 IAM 정책의 변경 사항에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 인증 및 권한 부여 제어가 영향을 받지 않게 하는 데 도움이 됩니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.
>
>   가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 결과를 생성합니다.

### 문제 해결

> **Note**
>
> 이러한 수정 단계에서 권장하는 필터 패턴은 CIS 지침의 필터 패턴과 다릅니다. 권장 필터는 IAM API 호출에서 발생하는 이벤트만 대상으로 합니다.

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventSource=iam.amazonaws.com) && (($.eventName=DeleteGroupPolicy) \|\| ($.eventName=DeleteRolePolicy) \|\| ($.eventName=DeleteUserPolicy) \|\| ($.eventName=PutGroupPolicy) \|\| ($.eventName=PutRo` |

| Field | 값 |
| --- | --- |
| | `lePolicy) \|\| ($.eventName=PutUserPolicy) \|\| ($.eventName=CreatePolicy) \|\| ($.eventName=DeletePolicy) \|\| ($.eventName=CreatePolicyVersion) \|\| ($.eventName=DeletePolicyVersion) \|\| ($.eventName=AttachRolePolicy) \|\| ($.eventName=DetachRolePolicy) \|\| ($.eventName=AttachUserPolicy) \|\| ($.eventName=DetachUserPolicy) \|\| ($.eventName=AttachGroupPolicy) \|\| ($.eventName=DetachGroupPolicy))}` |
| 메트릭 네임스페이스 | **LogMetrics** |
| 메트릭 값 | **1** |
| 기본값 | **0** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.5, CIS AWS 파운데이션 벤치마크 v1.4.0/4.5, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다.

CIS에서는 CloudTrail 구성 설정 변경에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 계정 내 활동에 대해 지속적인 가시성을 확보하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS 파운데이션 벤치마크 v1.4.0에서 컨트롤 4.5에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventName=CreateTrail) \|\| ($.eventName=UpdateTrail) \|\| ($.eventName=DeleteTrail) \|\| ($.eventName=StartLogging) \|\| ($.eventName=StopLogging)}` |
| 메트릭 네임스페이스 | **LogMetrics** |
| 메트릭 값 | **1** |
| 기본값 | **0** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.6, CIS AWS 파운데이션 벤치마크 v1.4.0/4.6, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다.

CIS에서는 실패한 콘솔 인증 시도에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 실패한 콘솔 로그인을 모니터링하면 자격 증명에 대한 Brute-Force 공격 시도를 감지하는 데 걸리는 리드 타임이 줄어 다른 이벤트 상관관계에서 사용할 수 있는 지표(예: 소스 IP)를 얻을 수 있습니다.

이 점검을 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS 파운데이션 벤치마크 v1.4.0에서 컨트롤 4.6에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.
>
>   가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에

서 평가된 제어에 대한 NO_DATA의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventName=ConsoleLogin) && ($.errorMessage="Failed authentication")}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |
| 기본값 | **`0`** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.7, CIS AWS 파운데이션 벤치마크 v1.4.0/4.7, NIST.800-171.r2 3.13.10, NIST.800-171.r2 3.13.16, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다.

CIS에서는 상태가 비활성화됨 또는 예약된 삭제로 변경된 고객 관리형 키에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 비활성화되거나 삭제된 키로 암호화된 데이터는 더 이상 액세스할 수 없습니다.

이 점검을 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.4.0에서 컨트롤 4.7에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된

정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다. `ExcludeManagementEventSources`에 `kms.amazonaws.com`이 포함된 경우에도 제어가 실패합니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.
>
>   가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.
>
> 경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventSource=kms.amazonaws.com) && (($.eventName=DisableKey) \|\| ($.eventName=ScheduleKeyDeletion))}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |
| 기본값 | **`0`** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *`your-metric-name`* 이 다음과 같을 때마다… | 크거나 같음 |

| Field | 값 |
| --- | --- |
| …보다 | **1** |

[CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.8, CIS AWS 파운데이션 벤치마크 v1.4.0/4.8, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다.

CIS에서는 S3 버킷 정책 변경 사항에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 민감한 S3 버킷에 관한 허용적인 정책을 감지하고 교정하는 데 걸리는 시간을 줄일 수 있습니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS 파운데이션 벤치마크 v1.4.0에서 컨트롤 4.8에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.

검사 조사 결과 다음과 같은 경우, FAILED 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우, NO_DATA의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 NO_DATA의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 ListSubscriptionsByTopic를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 WARNING 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.

3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventSource=s3.amazonaws.com) && (($.eventName=PutBucketAcl) \|\| ($.eventName=PutBucketPolicy) \|\| ($.eventName=PutBucketCors) \|\| ($.eventName=PutBucketLifecycle) \|\| ($.eventName=PutBucketReplication) \|\| ($.eventName=DeleteBucketPolicy) \|\| ($.eventName=DeleteBucketCors) \|\| ($.eventName=DeleteBucketLifecycle) \|\| ($.eventName=DeleteBucketReplication))}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |
| 기본값 | **`0`** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *`your-metric-name`* 이 다음과 같을 때마다... | 크거나 같음 |

| Field | 값 |
| --- | --- |
| …보다 | **1** |

[CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.9, CIS AWS 파운데이션 벤치마크 v1.4.0/4.9, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다.

CIS에서는 AWS Config 구성 설정 변경에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 계정 내 구성 항목에 대해 지속적인 가시성을 확보하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.4.0에서 제어 4.9에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.

- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우, NO_DATA의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 NO_DATA의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 조사 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.

3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventSource=config.amazonaws.com) && (($.eventName=StopConfigurationRecorder) \|\| ($.eventName=DeleteDeliveryChannel) \|\| ($.eventName=PutDeliveryChannel) \|\| ($.eventName=PutConfigurationRecorder))}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |
| 기본값 | **`0`** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *`your-metric-name`* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **`1`** |

[CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.10, CIS AWS 파운데이션 벤치마크 v1.4.0/4.10, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. 보안 그룹은 VPC에서 수신 및 발신 트래픽을 제어하는 상태 저장 패킷 필터입니다.

CIS에서는 보안 그룹 변경 사항에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 리소스 및 서비스가 의도치 않게 노출되는 일을 방지하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.4.0에서 컨트롤 4.10에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.

- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 조사 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventName=AuthorizeSecurityGroupIngress) \|\| ($.eventName=AuthorizeSecurityGroupE` |

| Field | 값 |
| --- | --- |
| | `gress) \|\| ($.eventName=Revok eSecurityGroupIngress) \|\| ($.eventName=RevokeSecurity GroupEgress) \|\| ($.eventN ame=CreateSecurityGroup) \|\| ($.eventName=DeleteSecurity Group)}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |
| 기본값 | **`0`** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *`your-metric-name`* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **`1`** |

[CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.11, CIS AWS 파운데이션 벤치마크 v1.4.0/4.11, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. NACL은 VPC에서 서브넷에 대한 수신 및 발신 트래픽을 제어하기 위한 상태 비저장 패킷 필터로 사용됩니다.

CIS에서는 NACL 변경 사항에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 AWS 리소스와 서비스가 의도치 않게 노출되지 않도록 할 수 있습니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.4.0의 컨트롤 4.11에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.
>
>   가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub

CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 조사 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventName=CreateNetworkAcl) \|\| ($.eventName=CreateNetworkAclEntry) \|\| ($.eventName=DeleteNetworkAcl) \|\| ($.eventName=DeleteNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclEntry) \|\| ($.eventName=ReplaceNetworkAclAssociation)}` |

| Field | 값 |
| --- | --- |
| 메트릭 네임스페이스 | **LogMetrics** |
| 메트릭 값 | **1** |
| 기본값 | **0** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.12, CIS AWS 파운데이션 벤치마크 v1.4.0/4.12, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. 네트워크 게이트웨이는 VPC 밖에 있는 대상에(서) 트래픽을 송수신하는 데 필요합니다.

CIS에서는 네트워크 게이트웨이 변경 사항에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 모든 수신 및 발신 트래픽이 제어된 경로를 통해 VPC 경계를 통과하게 하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.2의 컨트롤 4.12에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

> **Note**
>
> Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
> 검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.
>
> - 추적이 구성되어 있지 않습니다.
> - 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.
>
> 검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.
>
> - 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
> - 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.
>
> 가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 조사 결과를 생성합니다.

### 문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventName=CreateCustomerGateway) \|\| ($.eventName=DeleteCustomerGateway) \|\| ($.eventName=AttachInternetGateway) \|\| ($.eventName=CreateInternetGateway) \|\| ($.eventName=DeleteInternetGateway) \|\| ($.eventName=DetachInternetGateway)}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |
| 메트릭 값 | **`1`** |

| Field | 값 |
| --- | --- |
| 기본값 | **0** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.13, CIS AWS 파운데이션 벤치마크 v1.4.0/4.13, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

이 제어는 CloudTrail 로그를 CloudWatch Logs로 보내고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링하는지 여부를 확인합니다. 라우팅 테이블을 통해 네트워크 트래픽이 서브넷 간에, 그리고 네트워크 게이트웨이로 라우팅됩니다.

CIS에서는 라우팅 테이블 변경 사항에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 모든 VPC 트래픽이 예상 경로를 따라 흐르게 하는 데 도움이 됩니다.

**Note**

Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 조사 결과를 생성합니다.

문제 해결

> **Note**
>
> 이러한 수정 단계에서 권장하는 필터 패턴은 CIS 지침의 필터 패턴과 다릅니다. 권장 필터는 Amazon Elastic Compute Cloud(EC2) API 호출에서 발생하는 이벤트만 대상으로 합니다.

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventSource=ec2.amazonaws.com) && (($.eventName=CreateRoute) \|\| ($.eventName=CreateRouteTable) \|\| ($.eventName=ReplaceRoute) \|\| ($.eventName=ReplaceRouteTableAssociation) \|\| ($.eventName=DeleteRouteTable) \|\| ($.eventName=DeleteRoute) \|\| ($.eventName=DisassociateRouteTable))}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |

| Field | 값 |
| --- | --- |
| 메트릭 값 | **1** |
| 기본값 | **0** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/3.14, CIS AWS 파운데이션 벤치마크 v1.4.0/4.14, NIST.800-171.r2 3.3.1, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::Logs::MetricFilter`, `AWS::CloudWatch::Alarm`, `AWS::CloudTrail::Trail`, `AWS::SNS::Topic`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

CloudTrail 로그를 CloudWatch Logs로 전달하고 해당 메트릭 필터 및 경보를 설정하여 API 호출을 실시간으로 모니터링할 수 있습니다. 계정에 VPC가 한 개 이상 있을 수 있으므로 VPC 두 개 사이에 피어 연결을 생성하여 네트워크 트래픽이 VPC 간에 라우팅되게 할 수 있습니다.

CIS에서는 VPC 변경 사항에 대한 메트릭 필터 및 경보를 생성할 것을 권장합니다. 이러한 변경 사항을 모니터링하면 인증 및 권한 부여 제어가 영향을 받지 않게 하는 데 도움이 됩니다.

이 검사를 실행하기 위해 Security Hub CSPM은 사용자 지정 로직을 사용하여 CIS AWS Foundations Benchmark v1.4.0의 컨트롤 4.14에 대해 규정된 정확한 감사 단계를 수행합니다. CIS에 의해 규정된 정확한 메트릭 필터를 사용하지 않으면 이 제어가 실패합니다. 메트릭 필터에 추가 필드 또는 용어를 추가할 수 없습니다.

**Note**

Security Hub CSPM이이 제어에 대한 검사를 수행하면 현재 계정이 사용하는 CloudTrail 추적을 찾습니다. 이러한 추적은 다른 계정에 속한 조직 추적일 수 있습니다. 다중 리전 추적은 다른 리전을 기반으로 할 수도 있습니다.
검사 조사 결과 다음과 같은 경우, `FAILED` 조사 결과가 나타납니다.

- 추적이 구성되어 있지 않습니다.
- 현재 리전에 있고 현재 계정이 소유하고 있는 사용 가능한 추적은 제어 요구 사항을 충족하지 않습니다.

검사 결과 다음과 같은 경우, `NO_DATA`의 제어 상태가 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

  가장 좋은 방법은 조직 추적을 사용하여 조직의 여러 계정에서 이벤트를 로깅하는 것입니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations 관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 `NO_DATA`의 제어 상태가 나타납니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

경보를 받으려면 현재 계정이 참조된 Amazon SNS 주제를 소유하거나 `ListSubscriptionsByTopic`를 호출하여 Amazon SNS 주제에 액세스할 수 있어야 합니다. 그렇지 않으면 Security Hub CSPM이 컨트롤에 대한 `WARNING` 조사 결과를 생성합니다.

문제 해결

이 제어를 전달하려면 다음 단계에 따라 Amazon SNS 주제, AWS CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보를 생성합니다.

1. Amazon SNS 주제를 생성합니다. 이에 관한 지침은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요. 모든 CIS 경보를 수신하는 주제를 생성하고 해당 주제에 대한 구독을 하나 이상 생성하세요.
2. 모든 AWS 리전에 적용되는 CloudTrail 추적을 생성하세요. 이에 관한 지침은 AWS CloudTrail 사용자 설명서의 추적 생성을 참조하세요.

   CloudTrail 추적에 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 다음 단계에서 해당 로그 그룹에 대한 메트릭 필터를 생성합니다.
3. 메트릭 필터를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹에 대한 메트릭 필터 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 패턴 정의, 패턴 필터링 | `{($.eventName=CreateVpc) \|\| ($.eventName=DeleteVpc) \|\| ($.eventName=ModifyVpcAttribute) \|\| ($.eventName=AcceptVpcPeeringConnection) \|\| ($.eventName=CreateVpcPeeringConnection) \|\| ($.eventName=DeleteVpcPeeringConnection) \|\| ($.eventName=RejectVpcPeeringConnection) \|\| ($.eventName=AttachClassicLinkVpc) \|\| ($.eventName=DetachClassicLinkVpc) \|\| ($.eventName=DisableVpcClassicLink) \|\| ($.eventName=EnableVpcClassicLink)}` |
| 메트릭 네임스페이스 | **`LogMetrics`** |

| Field | 값 |
| --- | --- |
| 메트릭 값 | **1** |
| 기본값 | **0** |

4. 필터를 기반으로 경보를 생성합니다. 지침은 Amazon CloudWatch 사용 설명서의 로그 그룹 지표 필터를 기반으로 CloudWatch 경보 생성을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 조건, 임계값 유형 | 정적 |
| *your-metric-name* 이 다음과 같을 때마다… | 크거나 같음 |
| …보다 | **1** |

[CloudWatch.15] CloudWatch 경보에는 지정된 구성되어 있어야 합니다.

관련 요구 사항: 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, NIST.800-171.r2 3.14.6

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::CloudWatch::Alarm`

AWS Config 규칙: `cloudwatch-alarm-action-check`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| alarmActionRequired | 파라미터가 true로 설정되어 있고 경보 상태가 ALARM으로 변경될 때 작업이 경보에 포함되어 있는 경우, 제어가 PASSED 조사 결과를 생성합니다. | 부울 | 사용자 지정할 수 없음 | true |
| insufficientDataActionRequired | 파라미터가 true로 설정되어 있고 경보 상태가 INSUFFICIENT_DATA 으로 변경될 때 작업이 경보에 포함되어 있는 경우, 제어가 PASSED 조사 결과를 생성합니다. | 부울 | true 또는 false | false |
| okActionRequired | 파라미터가 true로 설정되어 있고 경보 상태가 OK으로 변경될 때 작업이 경보에 포함되어 있는 경우, 제어가 PASSED 조사 결과를 생성합니다. | 부울 | true 또는 false | false |

이 제어는 Amazon CloudWatch 경보에 ALARM 상태에 대해 구성된 작업이 하나 이상 있는지 확인합니다. ALARM 상태에 대해 활성화된 작업이 경보에 없으면 제어가 실패합니다. 필요에 따라 사용자 지정 파라미터 값을 포함시켜 INSUFFICIENT_DATA 또는 OK 상태에 대한 경보 작업도 요구할 수 있습니다.

> **Note**
>
> Security Hub CSPM은 CloudWatch 지표 경보를 기반으로이 제어를 평가합니다. 메트릭 경보는 지정된 작업이 구성된 복합 경보의 일부일 수 있습니다. 제어는 다음과 같은 경우, FAILED 조사 결과를 생성합니다.
>
> - 지정된 작업은 메트릭 경보에 대해 구성되지 않습니다.
> - 메트릭 경보는 지정된 작업이 구성된 복합 경보의 일부입니다.

이 제어는 CloudWatch 경보에 경보 작업이 구성되어 있는지 여부에 중점을 두는 반면, CloudWatch.17은 CloudWatch 경보 작업의 활성화 상태에 중점을 둡니다.

모니터링된 메트릭이 정의된 임계값을 벗어날 때 자동으로 경고하도록 CloudWatch 경보 작업을 권장합니다. 모니터링 경보를 통해 비정상적인 활동을 식별하고 경보가 특정 상태로 전환될 때 보안 및 운영 문제에 신속하게 대응할 수 있습니다. 가장 일반적인 유형의 경보 작업은 Amazon Simple Notification Service(SNS) 주제에 메시지를 전송하여 한 명 이상의 사용자에게 알리는 것입니다.

문제 해결

CloudWatch 경보가 지원하는 작업에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 경보 작업을 참조하세요.

[CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.

범주: 식별 > 로깅

관련 요구 사항: 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

심각도: 중간

리소스 유형: `AWS::Logs::LogGroup`

AWS Config 규칙: `cw-loggroup-retention-period-check`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `minRetentionTime` | CloudWatch 로그 그룹의 최소 보존 기간(일수) | Enum | `365`, `400`, `545`, `731`, `1827`, `3653` | `365` | |

이 제어는 Amazon CloudWatch 로그 그룹의 보존 기간이 지정된 일수 이상인지 확인합니다. 보존 기간이 지정된 수 미만인 경우, 제어가 실패합니다. 보존 기간 동안 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 365일을 사용합니다.

CloudWatch Logs는 확장성이 뛰어난 단일 서비스에서 모든 시스템, 애플리케이션 및 AWS 서비스 의 로그를 중앙 집중화합니다. CloudWatch Logs를 사용하여 Amazon Elastic Compute Cloud(EC2) 인스턴스, Amazon Route 53 및 기타 소스에서 로그 파일을 모니터링 AWS CloudTrail, 저장 및 액세스할 수 있습니다. 로그를 1년 이상 보관하면 로그 보존 표준을 준수하는 데 도움이 될 수 있습니다.

문제 해결

로그 보존 설정을 구성하려면 Amazon CloudWatch 사용 설명서의 CloudWatch Logs에서 로그 데이터 보존 변경을 참조하세요.

[CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.

범주: 감지 > 감지 서비스

관련 요구 사항: 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)

심각도: 높음

리소스 유형: `AWS::CloudWatch::Alarm`

AWS Config 규칙: `cloudwatch-alarm-action-enabled-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 CloudWatch 경보 조치가 활성화되었는지 확인합니다(`ActionEnabled`을 true로 설정해야 함). CloudWatch 경보에 대한 경보 작업이 비활성화되면 제어가 실패합니다.

> **Note**
>
> Security Hub CSPM은 CloudWatch 지표 경보를 기반으로이 제어를 평가합니다. 메트릭 경보는 경보 작업이 활성화된 복합 경보의 일부일 수 있습니다. 제어는 다음과 같은 경우, `FAILED` 조사 결과를 생성합니다.
>
> - 지정된 작업은 메트릭 경보에 대해 구성되지 않습니다.

- 메트릭 경보는 경보 작업이 활성화된 복합 경보의 일부입니다.

이 제어는 CloudWatch 경보 작업의 활성화 상태에 초점을 맞추는 반면 CloudWatch.15는 CloudWatch 경보에 ALARM 작업이 구성되어 있는지 여부에 중점을 둡니다.

경보 작업은 모니터링된 메트릭이 정의된 임계값을 벗어나면 자동으로 경고합니다. 경보 동작이 비활성화되면 경보 상태가 변경될 때 아무 작업도 실행되지 않으며 모니터링되는 메트릭의 변경에 대한 알림도 받지 않습니다. 보안 및 운영 문제에 신속하게 대응할 수 있도록 CloudWatch 경보 조치를 활성화하는 것이 좋습니다.

문제 해결

CloudWatch 경보 작업을 활성화하려면(콘솔)

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 경보 아래의 모든 경보를 선택합니다.
3. 동작을 활성화할 경보를 선택합니다.
4. 작업에서 경보 작업-새로운을 선택한 다음 활성화를 선택합니다.

CloudWatch 경보 설정에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 경보 조치를 참조하세요.

## CodeArtifact에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 AWS CodeArtifact서비스와 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::CodeArtifact::Repository`

AWS Config규칙: `tagged-codeartifact-repository` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS CodeArtifact리포지토리에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 리포지토리에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 리포지토리에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

CodeArtifact 리포지토리에 태그를 추가하려면 AWS CodeArtifact 사용 설명서의 CodeArtifact에서 리포지토리 태그 지정을 참조하세요.

## CodeBuild에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 AWS CodeBuild서비스와 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 SA-3, PCI DSS v3.2.1/8.2.1, PCI DSS v4.0.1/8.3.2

범주: 보호 > 보안 개발

심각도: 심각

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-source-repo-url-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS CodeBuild프로젝트 Bitbucket 소스 리포지토리 URL에 개인 액세스 토큰 또는 사용자 이름 및 암호가 포함되어 있는지 확인합니다. 이 제어는 Bitbucket 소스 리포지토리 URL에 개인 액세스 토큰 또는 사용자 이름 및 암호가 포함되어 있는지 확인합니다.

> **Note**
>
> 이 제어는 CodeBuild 빌드 프로젝트의 기본 소스와 보조 소스를 모두 평가합니다. 프로젝트 소스에 대한 자세한 내용은 AWS CodeBuild 사용 설명서의 여러 입력 소스 및 출력 아티팩트 샘플을 참조하세요.

로그인 자격 증명은 일반 텍스트로 저장 또는 전송되거나 저장소 URL에 표시되어서는 안 됩니다. 개인 액세스 토큰 또는 로그인 자격 증명 정보 대신 CodeBuild의 소스 공급자에 액세스하고 Bitbucket 리포지토리 위치 경로만 포함하도록 소스 리포지토리 URL을 변경해야 합니다. 개인 액세스 토큰 또는 로그인 보안 인증을 사용하면 자격 증명이 의도하지 않은 데이터 노출 및 무단 액세스에 노출될 수 있습니다.

문제 해결

OAuth를 사용하도록 CodeBuild 프로젝트를 업데이트할 수 있습니다.

CodeBuild 프로젝트 소스에서 기본 인증/(GitHub) 개인 액세스 토큰을 제거하려면

1. https://console.aws.amazon.com/codebuild/에서 CodeBuild 콘솔을 엽니다.
2. 개인 액세스 토큰 또는 사용자 이름과 암호가 포함된 빌드 프로젝트를 선택합니다.
3. 편집에서 소스를 선택합니다.
4. GitHub/Bitbucket에서 연결 해제를 선택합니다.
5. OAuth를 사용하여 연결을 선택한 후 GitHub/Bitbucket에 연결을 선택합니다.
6. 메시지가 표시되면 적절한 권한 부여를 선택합니다.
7. 필요에 따라 리포지토리 URL 및 추가 구성 설정을 다시 구성합니다.
8. 소스 업데이트를 선택합니다.

자세한 내용은 AWS CodeBuild 사용 설명서의 CodeBuild 사용 사례 기반 샘플을 참조하세요.

[CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 보안 개발

심각도: 심각

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-envvar-awscred-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 프로젝트에 환경 변수 `AWS_ACCESS_KEY_ID` 및 `AWS_SECRET_ACCESS_KEY`가 포함되었는지 확인합니다.

인증 보안 인증 정보 `AWS_ACCESS_KEY_ID` 및 `AWS_SECRET_ACCESS_KEY`를 일반 텍스트로 저장해서는 안 됩니다. 이로 인해 의도하지 않은 데이터 노출 및 무단 액세스가 발생할 수 있습니다.

문제 해결

CodeBuild 프로젝트에서 환경 변수를 제거하려면 AWS CodeBuild 사용 설명서의 AWS CodeBuild에서 빌드 프로젝트 설정 변경을 참조하세요. 환경 변수에 대해 아무것도 선택되지 않았는지 확인하세요.

Parameter Store 또는 AWS Systems Manager에 민감한 값을 가진 환경 변수를 저장한 AWS Secrets Manager다음 빌드 사양에서 검색할 수 있습니다. 지침은 AWS CodeBuild 사용 설명서의 환경 섹션에서 중요라고 표시된 상자를 참조하세요.

[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 낮음

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-s3-logs-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS CodeBuild프로젝트에 대한 Amazon S3 로그가 암호화되었는지 확인합니다. CodeBuild 프로젝트의 S3 로그에 대해 암호화가 비활성화되면 제어가 실패합니다.

저장 데이터 암호화는 데이터 주위에 액세스 관리 계층을 추가하기 위해 권장되는 모범 사례입니다. 저장 로그를 암호화하면에서 인증하지 않은 사용자가 디스크에 저장된 데이터에 AWS액세스할 위험이 줄어듭니다. 이는 승인되지 않은 사용자가 데이터에 액세스하는 능력을 제한하기 위해 또 다른 액세스 제어 세트를 추가합니다.

문제 해결

CodeBuild 프로젝트 S3 로그의 암호화 설정을 변경하려면 AWS CodeBuild 사용 설명서의 AWS CodeBuild에서 빌드 프로젝트 설정 변경을 참조하세요.

[CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 CodeBuild 프로젝트 환경에 S3 또는 CloudWatch 로그가 활성화된 로그 옵션이 하나 이상 있는지 확인합니다. CodeBuild 프로젝트 환경에 하나 이상의 로그 옵션이 활성화되어 있지 않으면 이 제어가 실패합니다.

보안 관점에서 볼 때 로깅은 보안 사고 발생 시 향후 포렌식 활동을 가능하게 하는 중요한 기능입니다. CodeBuild 프로젝트의 이상 징후를 위협 탐지와 연관시키면 위협 탐지의 정확성에 대한 신뢰도를 높일 수 있습니다.

문제 해결

CodeBuild 프로젝트 로그 설정을 구성하는 방법에 대한 자세한 내용은 CodeBuild 사용 설명서의 빌드 프로젝트 만들기(콘솔)를 참조하세요.

[CodeBuild.5] CodeBuild 프로젝트 환경에서는 권한 모드가 활성화되어서는 안 됩니다.

> **Important**
>
> Security Hub CSPM은 2024년 4월에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그 단원을 참조하십시오.

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::CodeBuild::Project`

AWS Config 규칙: `codebuild-project-environment-privileged-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS CodeBuild프로젝트 환경에 권한 모드가 활성화 또는 비활성화되어 있는지 확인합니다. CodeBuild 프로젝트 환경에 권한 모드가 활성화되어 있는 경우, 제어가 실패합니다.

기본적으로 Docker 컨테이너는 모든 디바이스에 대한 액세스를 허용하지 않습니다. 권한 모드는 빌드 프로젝트의 Docker 컨테이너에 모든 디바이스에 대한 액세스 권한을 부여합니다. 값 `true`을 사용하여 `privilegedMode`를 설정하면 Docker 대몬(daemon)을 Docker 컨테이너 내에서 실행할 수 있습니다. Docker 대몬(daemon)은 Docker API 요청을 수신하고 이미지, 컨테이너, 네트워크 및 볼륨과 같은 Docker 객체를 관리합니다. 이 파라미터는 빌드 프로젝트가 Docker 이미지를 빌드하는 데 사용되는 경우에만 true로 설정해야 합니다. 그렇지 않으면 Docker API와 컨테이너의 기본 하드웨어에 대한 의도하지 않은 액세스를 방지하기 위해 이 설정을 비활성화해야 합니다. `privilegedMode`를 `false`로 설정하면 중요한 리소스가 변조 및 삭제되지 않도록 보호하는 데 도움이 됩니다.

문제 해결

CodeBuild 프로젝트 환경 설정을 구성하려면 CodeBuild 사용 안내서의 빌드 프로젝트 만들기(콘솔)를 참조하세요. 환경 섹션에서 권한 설정을 선택하지 마세요.

[CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::CodeBuild::ReportGroup`

AWS Config 규칙: `codebuild-report-group-encrypted-at-rest`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Simple Storage Service(Amazon S3) 버킷으로 내보내는 AWS CodeBuild보고서 그룹의 테스트 결과가 저장 시 암호화되는지 확인합니다. 복구 시점이 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 저장 데이터를 암호화하면 기밀성을 보호할 수 있으므로 권한이 없는 사용자가 데이터에 액세스할 수 있는 위험이 줄어듭니다.

문제 해결

S3로 보고서 그룹 내보내기를 암호화하려면 AWS CodeBuild 사용 설명서의 보고서 그룹 업데이트를 참조하세요.

## Amazon CodeGuru Profiler에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon CodeGuru Profiler 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::CodeGuruProfiler::ProfilingGroup`

AWS Config 규칙: `codeguruprofiler-profiling-group-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon CodeGuru Profiler 프로파일링 그룹에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 프로파일링 그룹에 태그 키가 없거나 파

라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 프로파일링 그룹에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

CodeGuru Profiler 프로파일링 그룹에 태그를 추가하려면 Amazon CodeGuru Profiler 사용 설명서의 프로파일링 그룹에 태그 지정을 참조하세요.

## Amazon CodeGuru Reviewer에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon CodeGuru Reviewer 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::CodeGuruReviewer::RepositoryAssociation`

AWS Config 규칙: `codegurureviewer-repository-association-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon CodeGuru Reviewer 리포지토리 연결에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 리포지토리 연결에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 리포지토리 연결에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

CodeGuru Reviewer 리포지토리 연결에 태그를 추가하려면 Amazon CodeGuru Reviewer 사용 설명서의 리포지토리 연결에 태그 지정을 참조하세요.

## Amazon Cognito에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon Cognito 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::Cognito::UserPool`

AWS Config 규칙: cognito-user-pool-advanced-security-enabled

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `SecurityMode` | 제어가 확인하는 위협 방지 적용 모드입니다. | 문자열 | `AUDIT`, `ENFORCED` | `ENFORCED` |

이 제어는 Amazon Cognito 사용자 풀에 위협 방지가 활성화되고 표준 인증을 위한 적용 모드가 전체 기능으로 설정되어 있는지 확인합니다. 사용자 풀에 위협 방지 기능이 비활성화되어 있거나 표준 인증을 위한 적용 모드가 전체 기능으로 설정되지 않은 경우 제어가 실패합니다. 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 표준 인증을 `ENFORCED` 위해 전체 함수로 설정된 적용 모드에의 기본값을 사용합니다.

Amazon Cognito 사용자 풀을 생성한 후 위협 방지를 활성화하고 다양한 위험에 대응하여 취하는 조치를 사용자 지정할 수 있습니다. 또는 감사 모드를 사용하여 보안 완화를 적용하지 않고 탐지된 위험에

대한 지표를 수집할 수 있습니다. 감사 모드에서 위협 방지는 Amazon CloudWatch에 지표를 게시합니다. Amazon Cognito가 첫 번째 이벤트를 생성한 후에 지표를 볼 수 있습니다.

문제 해결

Amazon Cognito 사용자 풀에 대한 위협 방지 활성화에 대한 자세한 내용은 Amazon Cognito 개발자 안내서의 위협 방지를 사용한 고급 보안을 참조하세요.

[Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::Cognito::IdentityPool`

AWS Config 규칙: cognito-identity-pool-unauth-access-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Cognito ID 풀이 인증되지 않은 ID를 허용하도록 구성되어 있는지 확인합니다. ID 풀에서 게스트 액세스가 활성화되어 있는 경우(`AllowUnauthenticatedIdentities` 파라미터가 `true`로 설정됨) 제어가 실패합니다.

Amazon Cognito 자격 증명 풀이 인증되지 않은 자격 증명을 허용하는 경우 자격 증명 풀은 자격 증명 공급자(게스트)를 통해 인증하지 않은 사용자에게 임시 AWS 자격 증명을 제공합니다. 이렇게 하면 AWS 리소스에 대한 익명 액세스를 허용하므로 보안 위험이 발생합니다. 게스트 액세스를 비활성화하면 제대로 인증된 사용자만 AWS 리소스에 액세스할 수 있으므로 무단 액세스 및 잠재적 보안 침해의 위험이 줄어듭니다. 모범 사례로 ID 풀은 지원되는 ID 제공업체를 통해 인증하도록 요구해야 합니다. 인증되지 않은 액세스가 필요한 경우 인증되지 않은 ID의 권한을 신중하게 제한하고 해당 사용을 정기적으로 검토하고 모니터링하는 것이 중요합니다.

문제 해결

Amazon Cognito ID 풀에서 게스트 액세스를 비활성화하는 방법에 대한 자세한 내용은 Amazon Cognito 개발자 안내서의 게스트 액세스 활성화 또는 비활성화를 참조하세요.

[Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::Cognito::UserPool`

AWS Config 규칙: cognito-user-pool-password-policy-check

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `minLength` | 암호가 포함해야 할 최소 문자 수입니다. | Integer | 8~99 | 8 |
| `requireLowercase` | 암호에 소문자가 1개 이상이어야 합니다. | 부울 | `True`, `False` | `True` |
| `requireUppercase` | 암호에 대문자가 1개 이상이어야 합니다. | 부울 | `True`, `False` | `True` |
| `requireNumbers` | 암호에 숫자가 1개 이상이어야 합니다. | 부울 | `True`, `False` | `True` |
| `requireSymbols` | 암호에 기호가 1개 이상이어야 합니다. | 부울 | `True`, `False` | `True` |
| `temporaryPasswordValidity` | 암호가 만료까지 존재할 수 있는 최대 일수입니다. | Integer | 1~365 | 7 |

이 제어는 Amazon Cognito 사용자 풀의 암호 정책이 암호 정책의 권장 설정에 따른 강력한 암호를 사용하도록 요구하는지 여부를 확인합니다. 사용자 풀의 암호 정책이 강력한 암호를 요구하지 않는 경우 제어가 실패합니다. 선택적으로 제어가 확인하는 정책 설정에 사용자 지정 값을 지정할 수 있습니다.

강력한 암호는 Amazon Cognito 사용자 풀의 보안 모범 사례입니다. 약한 암호를 사용하면 사용자의 자격 증명이 암호를 추측하여 데이터에 액세스하려고 시도하는 시스템에 노출될 수 있습니다. 인터넷에 공개된 애플리케이션의 경우 특히 그렇습니다. 암호 정책은 사용자 디렉터리 보안의 핵심 요소입니다. 암호 정책을 사용하면 사용자의 보안 표준 및 요구 사항을 준수하는 암호 복잡성 및 기타 설정을 요구하도록 사용자 풀을 구성할 수 있습니다.

문제 해결

Amazon Cognito 사용자 풀의 암호 정책을 생성하거나 업데이트하는 방법에 대한 자세한 내용은 Amazon Cognito 개발자 안내서의 사용자 풀 암호 요구 사항 추가를 참조하세요.

[Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::Cognito::UserPool`

AWS Config 규칙: cognito-userpool-cust-auth-threat-full-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Cognito 사용자 풀에 사용자 지정 인증을 위해 전체 함수로 설정된 적용 모드로 위협 방지가 활성화되어 있는지 확인합니다. 사용자 풀에 위협 방지 기능이 비활성화되어 있거나 적용 모드가 사용자 지정 인증을 위한 전체 함수로 설정되지 않은 경우 제어가 실패합니다.

위협 방지는 이전에 고급 보안 기능으로 불렸으며, 사용자 풀에서 원치 않는 활동에 대한 모니터링 도구 세트이며 잠재적으로 악의적인 활동을 자동으로 종료하는 구성 도구입니다. Amazon Cognito 사용자 풀을 생성한 후 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지를 활성화하고 다양한 위험에 대응하여 수행되는 작업을 사용자 지정할 수 있습니다. 전체 기능 모드에는 원치 않는 활동 및 손상된 암호를 감지하기 위한 자동 반응 세트가 포함되어 있습니다.

문제 해결

Amazon Cognito 사용자 풀에 대한 위협 방지 활성화에 대한 자세한 내용은 Amazon Cognito 개발자 안내서의 위협 방지를 사용한 고급 보안을 참조하세요.

[Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.

범주: 보호 > 보안 액세스 관리 > 다중 인증

심각도: 중간

리소스 유형: `AWS::Cognito::UserPool`

AWS Config 규칙: cognito-user-pool-mfa-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 암호 전용 로그인 정책으로 구성된 Amazon Cognito 사용자 풀에 다중 인증(MFA)이 활성화되어 있는지 확인합니다. 암호 전용 로그인 정책으로 구성된 사용자 풀에 MFA가 활성화되어 있지 않으면 제어가 실패합니다.

다중 인증(MFA)은 사용자가 알고 있는 요소(일반적으로 사용자 이름 및 암호)에 인증 요소가 있는 요소를 추가합니다. 페더레이션 사용자의 경우 Amazon Cognito는 자격 증명 공급자(IdP)에 인증을 위임하며 추가 인증 요소를 제공하지 않습니다. 그러나 암호 인증을 사용하는 로컬 사용자가 있는 경우 사용자 풀에 대해 MFA를 구성하면 보안이 향상됩니다.

> **Note**
>
> 암호 없는 요소로 로그인하는 페더레이션 사용자 및 사용자에게는 이 제어가 적용되지 않습니다.

문제 해결

Amazon Cognito 사용자 풀에 대해 MFA를 구성하는 방법에 대한 자세한 내용은 Amazon Cognito 개발자 안내서의 사용자 풀에 MFA 추가를 참조하세요.

[Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 중간

리소스 유형: `AWS::Cognito::UserPool`

AWS Config 규칙: cognito-user-pool-deletion-protection-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Cognito 사용자 풀에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 사용자 풀에 대해 삭제 방지가 비활성화된 경우 제어가 실패합니다.

삭제 방지 기능은 사용자 풀이 실수로 삭제되지 않도록 하는 데 도움이 됩니다. 삭제 방지 기능을 사용하여 사용자 풀을 구성하면 사용자가 풀을 삭제할 수 없습니다. 삭제 방지 기능을 사용하면 먼저 풀을 수정하고 삭제 방지 기능을 비활성화하지 않는 한 사용자 풀 삭제를 요청할 수 없습니다.

문제 해결

Amazon Cognito 사용자 풀에 대한 삭제 보호를 구성하려면 Amazon Cognito 개발자 안내서의 사용자 풀 삭제 보호를 참조하세요.

## 에 대한 Security Hub CSPM 제어 AWS Config

이러한 Security Hub CSPM 제어는 AWS Config 서비스와 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다.

> **Note**
>
> Security Hub CSPM 및 Security Hub가 활성화된 경우 Config.1 규칙의 상태는 항상 PASSED 입니다. 이는 Security Hub CSPM이 서비스 연결 구성 레코더를 통해 구성 항목에 직접 액세스할 수 있기 때문입니다. 내부 서비스 연결 구성 레코더가 AWS Config 서비스 연결 역할로 자동으로 생성되므로이 제어의 파라미터는 적용할 수 없습니다. 자세한 내용은 서비스 연결 구성 레코더 사용 단원을 참조하십시오.
> 멀티클라우드 제어(예: Azure 제어) 및 관련 리소스 레코딩은 Config.1 평가에 고려되지 않습니다. 멀티클라우드 표준은 Security Hub 활성화 상태에 관계없이 CSPM 멀티클라우드 커넥터가 자동으로 설정하는 내부 서비스 연결 구성 레코더를 항상 사용합니다. 멀티클라우드 레코딩은 커넥터에서 완전히 관리되므로 Config.1 규정 준수 상태에는 영향을 주지 않습니다. Config.1은 AWS 리소스 기록 구성만 평가합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/3.3, CIS AWS 파운데이션 벤치마크 v1.2.0/2.5, CIS AWS 파운데이션 벤치마크 v1.4.0/3.5, CIS AWS 파운데이션 벤치마크 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

범주: 식별 > 인벤토리

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: 없음(사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `includeConfigServiceLinkedRoleCheck` | 파라미터가 로 설정된 경우 제어는가 서비스 연결 역할을 AWS Config 사용하는지 여부를 평가하지 않습니다`false`. | 부울 | `true` 또는 `false` | `true` |

이 제어 AWS Config 는 현재의 계정에서가 활성화되었는지 확인하고 AWS 리전, 현재 리전에서 활성화된 제어에 해당하는 모든 리소스를 기록하고, 서비스 연결 AWS Config 역할을 사용합니다. 서비스 연결 역할의 이름은 바로 AWSServiceRoleForConfig입니다. 서비스 연결 역할을 사용하지 않고 `includeConfigServiceLinkedRoleCheck` 파라미터를 로 설정하지 않으면 다른 역할에 리소스를 정확하게 기록 AWS Config 하는 데 필요한 권한이 없을 수 있으므로 `false`제어가 실패합니다.

AWS Config 서비스는 계정에서 지원되는 AWS 리소스의 구성 관리를 수행하고 로그 파일을 제공합니다. 기록된 정보에는 구성 항목(AWS 리소스), 구성 항목 간의 관계, 리소스 내 구성 변경 사항이 포함됩니다. 글로벌 리소스는 모든 리전에서 사용할 수 있는 리소스입니다.

컨트롤은 다음과 같이 평가됩니다.

- 현재 리전이 집계 리전으로 설정된 경우 제어는 AWS Identity and Access Management (IAM) 글로벌 리소스가 기록된 경우에만 `PASSED` 결과를 생성합니다(필요한 제어를 활성화한 경우).
- 현재 리전이 연결된 리전으로 설정된 경우, 제어는 IAM 글로벌 리소스가 기록되는지 여부를 평가하지 않습니다.
- 현재 리전이 집계자에 없거나 교차 리전 집계가 계정에 설정되지 않은 경우, 제어는 IAM 글로벌 리소스가 기록된 경우에만 `PASSED` 조사 결과를 생성합니다(필요한 제어를 활성화한 경우).

제어 결과는 AWS Config에서 리소스 상태의 변화에 대한 일일 또는 지속적 레코딩을 선택하든 영향을 받지 않습니다. 하지만 새로운 제어의 자동 활성화를 구성했거나 새로운 제어를 자동으로 활성화하는 중앙 구성 정책이 있는 경우, 새로운 제어가 릴리스될 때 이 제어의 결과가 변경될 수 있습니다. 이러한

경우 모든 리소스를 기록하지 않는 경우, PASSED 조사 결과를 받으려면 새로운 제어와 연결된 리소스에 대한 레코딩을 구성해야 합니다.

Security Hub CSPM 보안 검사는 모든 리전 AWS Config 에서를 활성화하고 필요한 제어에 대한 리소스 기록을 구성하는 경우에만 의도한 대로 작동합니다.

> **Note**
>
> Config.1에서는 Security Hub CSPM을 사용하는 모든 리전에서를 AWS Config 활성화해야 합니다.
> Security Hub CSPM은 리전 서비스이므로이 제어에 대해 수행된 검사는 계정의 현재 리전만 평가합니다.
> 각 리전에서 IAM 글로벌 리소스에 대한 보안 점검을 확인하려면 글로벌 리소스를 기록해야 합니다. IAM 글로벌 리소스가 기록되지 않은 리전은 IAM 글로벌 리소스를 확인하는 제어에 대한 기본 PASSED 조사 결과를 받게 됩니다. IAM 글로벌 리소스는 전체적으로 동일하므로 홈 리전에만 IAM 글로벌 리소스를 기록하는 AWS 리전것이 좋습니다(계정에서 교차 리전 집계가 활성화된 경우). IAM 리소스는 글로벌 리소스 레코딩이 활성화된 리전에만 레코딩됩니다.
> 에서 AWS Config 지원하는 IAM 전역적으로 기록된 리소스 유형은 IAM 사용자, 그룹, 역할 및 고객 관리형 정책입니다. 글로벌 리소스 기록이 꺼져 있는 리전에서 이러한 리소스 유형을 확인하는 Security Hub CSPM 제어를 비활성화하는 것을 고려할 수 있습니다. 자세한 내용은 Security Hub CSPM에서 비활성화가 권장되는 제어 단원을 참조하십시오.

문제 해결

집계자의 일부가 아닌 홈 리전 및 리전에서 IAM 글로벌 리소스가 필요한 제어를 활성화한 경우, IAM 글로벌 리소스를 포함하여 현재 리전에서 활성화된 제어에 필요한 모든 리소스를 기록합니다.

연결된 리전에서는 현재 리전에서 활성화된 제어에 해당하는 모든 리소스를 AWS Config 기록하는 한 모든 기록 모드를 사용할 수 있습니다. 연결된 리전에서 IAM 글로벌 리소스의 기록을 요구하는 제어를 활성화한 경우, FAILED 조사 결과를 수신하지 못합니다(다른 리소스의 기록으로 충분함).

조사 결과의 Compliance 객체 내 StatusReasons 필드는 이 제어에 대해 실패 조사 결과가 있는 이유를 파악하는 데 도움이 될 수 있습니다. 자세한 내용은 제어 조사 결과에 대한 규정 준수 세부 정보 단원을 참조하십시오.

각 제어에 대해 기록해야 하는 리소스 목록은 제어 조사 결과에 필요한 AWS Config리소스 섹션을 참조하세요. 리소스 레코딩 활성화 AWS Config 및 구성에 대한 일반적인 내용은 섹션을 참조하세요Security Hub CSPM AWS Config 에 대한 활성화 및 구성.

## Amazon Connect에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon Connect 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::CustomerProfiles::ObjectType`

AWS Config 규칙: `customerprofiles-object-type-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Connect Customer Profiles 객체 유형에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 객체 유형에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 객체 유형에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는

데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

Customer Profiles 객체 유형에 태그를 추가하려면 고객 연결 관리자 안내서의 Amazon Connect Customer의 리소스에 태그 추가를 참조하세요.

[Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Connect::Instance`

AWS Config규칙: connect-instance-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Connect Customer 인스턴스가 흐름 로그를 생성하고 Amazon CloudWatch 로그 그룹에 저장하도록 구성되어 있는지 확인합니다. Connect Customer 인스턴스가 CloudWatch 로그 그룹에 흐름 로그를 생성하고 저장하도록 구성되지 않은 경우 제어가 실패합니다.

Amazon Connect 고객 흐름 로그는 Amazon Connect 고객 흐름의 이벤트에 대한 실시간 세부 정보를 제공합니다. 흐름은 Amazon Connect 고객 센터의 고객 경험을 처음부터 끝까지 정의합니다. 기본적으로 새 Amazon Connect Customer 인스턴스를 생성하면 Amazon CloudWatch 로그 그룹이 자동으로

생성되어 인스턴스에 대한 흐름 로그를 저장합니다. 흐름 로그는 흐름을 분석하고, 오류를 찾고, 운영 지표를 모니터링하는 데 도움이 될 수 있습니다. 흐름에서 발생할 수 있는 특정 이벤트에 대한 알림을 설정할 수도 있습니다.

문제 해결

Amazon Connect 고객 인스턴스에 대한 흐름 로그 활성화에 대한 자세한 내용은 고객 Amazon Connect 관리자 안내서의 Amazon CloudWatch 로그 그룹에서 Amazon Connect 고객 흐름 로그 활성화를 참조하세요.

## Amazon Data Firehose에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon Data Firehose 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::KinesisFirehose::DeliveryStream`

AWS Config 규칙: `kinesis-firehose-delivery-stream-encrypted`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Data Firehose 전송 스트림이 서버 측 암호화로 저장 시 암호화되는지 여부를 확인합니다. Firehose 전송 스트림이 서버 측 암호화를 통해 저장 시 암호화되지 않으면 이 제어가 실패합니다.

서버 측 암호화는 AWS Key Management Service()에서 생성된 키를 사용하여 저장되기 전에 데이터를 자동으로 암호화하는 Amazon Data Firehose 전송 스트림의 기능입니다AWS KMS. 데이터는 Data Firehose 스트림 스토리지 계층에 쓰여지기 전에 암호화되고 스토리지에서 검색된 후 해독됩니다. 이렇게 하면 규제 요구 사항을 충족시키고 데이터 보안을 강화할 수 있습니다.

문제 해결

Firehose 전송 스트림에서 서버 측 암호화를 활성화하려면 Amazon Data Firehose 개발자 안내서의 Amazon Data Firehose의 데이터 보호를 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Database Migration Service

이러한 AWS Security Hub CSPM제어는 AWS Database Migration Service(AWS DMS) 및 AWS DMS 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::DMS::ReplicationInstance`

AWS Config 규칙: dms-replication-not-public

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS DMS복제 인스턴스가 퍼블릭인지 확인합니다. 이를 위해 `PubliclyAccessible` 필드의 값을 검사합니다.

프라이빗 복제 인스턴스에는 복제 네트워크 외부에서 액세스할 수 없는 프라이빗 IP 주소가 있습니다. 소스 및 대상 데이터베이스가 동일한 네트워크에 있는 경우, 복제 인스턴스에는 사설 IP 주소가 있어야 합니다. 또한 네트워크는 VPN Direct Connect또는 VPC 피어링을 사용하여 복제 인스턴스의 VPC에 연결되어야 합니다. 퍼블릭 및 프라이빗 복제 인스턴스에 대해 자세히 알아보려면 AWS Database Migration Service 사용 설명서의 퍼블릭 및 프라이빗 복제 인스턴스를 참조하세요.

또한 AWS DMS인스턴스 구성에 대한 액세스가 승인된 사용자로만 제한되도록 해야 합니다. 이렇게 하려면 사용자의 IAM 권한을 제한하여 AWS DMS설정 및 리소스를 수정합니다.

문제 해결

DMS 복제 인스턴스를 생성한 후에는 해당 인스턴스의 퍼블릭 액세스 설정을 변경할 수 없습니다. 퍼블릭 액세스 설정을 변경하려면 현재 인스턴스를 삭제한 다음 다시 생성하세요. 퍼블릭 액세스 가능 옵션을 선택하지 마세요.

[DMS.2] DMS 인증서에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DMS::Certificate`

AWS Config규칙: `tagged-dms-certificate` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS DMS인증서에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 인증서에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 인증서에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검

색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

DMS 인증서에 태그를 추가하려면 AWS Database Migration Service 사용 설명서의 에서 리소스 태깅 AWS Database Migration Service을 참조하세요.

[DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DMS::EventSubscription`

AWS Config규칙: `tagged-dms-eventsubscription` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS DMS이벤트 구독에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 이벤트 구독에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 이벤트 구독에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

DMS 이벤트 구독에 태그를 추가하려면 AWS Database Migration Service 사용 설명서의 리소스 태깅 AWS Database Migration Service을 참조하세요.

[DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: AWS::DMS::ReplicationInstance

AWS Config규칙: tagged-dms-replicationinstance (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS DMS복제 인스턴스에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 복제 인스턴스에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 복제 인스턴스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

DMS 복제 인스턴스에 태그를 추가하려면 AWS Database Migration Service 사용 설명서의 리소스 태깅AWS Database Migration Service 섹션을 참조하세요.

[DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DMS::ReplicationSubnetGroup`

AWS Config규칙: `tagged-dms-replicationsubnetgroup` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS DMS복제 서브넷 그룹에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 복제 서브넷 그룹에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 복제 서브넷 그룹에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

DMS 복제 서브넷 그룹에 태그를 추가하려면 AWS Database Migration Service 사용 설명서의 AWS Database Migration Service에서 리소스 태깅을 참조하세요.

[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::DMS::ReplicationInstance`

AWS Config 규칙: dms-auto-minor-version-upgrade-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS DMS복제 인스턴스에 대해 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. DMS 복제 인스턴스에 자동 마이너 버전 업그레이드가 활성화되어 있지 않으면 제어가 실패합니다.

DMS는 지원되는 각 복제 엔진에 대한 자동 마이너 버전 업그레이드를 제공하여 복제 인스턴스를 최신 상태로 유지합니다. 마이너 버전은 새로운 소프트웨어 기능, 버그 수정, 보안 패치 및 성능 개선을 도입할 수 있습니다. DMS 복제 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하면 유지 관리 기간 중에 마이너 업그레이드가 자동으로 적용되거나 변경 사항 즉시 적용 옵션을 선택한 경우, 즉시 적용됩니다.

문제 해결

DMS 복제 인스턴스에서 자동 마이너 버전 업그레이드를 활성화하려면 AWS Database Migration Service 사용 설명서의 복제 인스턴스 수정을 참조하세요.

[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::DMS::ReplicationTask`

AWS Config 규칙: dms-replication-task-targetdb-logging

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 DMS 복제 작업 `TARGET_APPLY` 및 `TARGET_LOAD`에 대해 최소 심각도 수준 `LOGGER_SEVERITY_DEFAULT`으로 로깅이 활성화되어 있는지 확인합니다. 이러한 작업에 대한 로깅이 활성화되지 않았거나 최소 심각도 수준이 `LOGGER_SEVERITY_DEFAULT`보다 낮으면 제어가 실패합니다.

DMS에서는 마이그레이션 프로세스 중에 Amazon CloudWatch를 사용하여 정보를 로그합니다. 로깅 작업 설정을 사용하면 기록할 구성 요소 활동과 기록할 정보의 양을 지정할 수 있습니다. 다음 작업에 대한 로깅을 지정해야 합니다.

- `TARGET_APPLY` – 데이터 및 데이터 정의 언어(DDL) 문이 대상 데이터베이스에 적용됩니다.
- `TARGET_LOAD` – 데이터가 대상 데이터베이스에 로드됩니다.

로깅은 모니터링, 문제 해결, 감사, 성능 분석, 오류 탐지, 복구, 기간별 분석 및 보고를 가능하게 함으로써 DMS 복제 작업에서 중요한 역할을 합니다. 이를 통해 데이터 무결성을 유지하고 규제 요구 사항을 준수하면서 데이터베이스 간에 데이터를 성공적으로 복제할 수 있습니다. 문제 해결 중에 이러한 구성 요소에는 `DEFAULT` 이외의 로깅 수준이 거의 필요하지 않습니다. 지원에서 특별히 변경을 요청하지 않는 한 이러한 구성 요소에 대한 로깅 수준을 `DEFAULT`으로 유지하는 것이 좋습니다. 최소 로깅 수준 `DEFAULT`을 사용하면 정보 메시지, 경고 및 오류 메시지가 로그에 기록됩니다. 이 제어는 이전 복제 작업에 대한 로깅 수준이 `LOGGER_SEVERITY_DEFAULT`, `LOGGER_SEVERITY_DEBUG` 또는 `LOGGER_SEVERITY_DETAILED_DEBUG` 중 하나 이상인지 확인합니다.

문제 해결

대상 데이터베이스 DMS 복제 작업에 대한 로깅을 활성화하려면 AWS Database Migration Service사용 설명서의 AWS DMS작업 로그 보기 및 관리를 참조하세요.

[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::DMS::ReplicationTask`

AWS Config 규칙: dms-replication-task-sourcedb-logging

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 DMS 복제 작업 `SOURCE_CAPTURE` 및 `SOURCE_UNLOAD`에 대해 최소 심각도 수준 `LOGGER_SEVERITY_DEFAULT`으로 로깅이 활성화되어 있는지 확인합니다. 이러한 작업에 대한 로깅이 활성화되지 않았거나 최소 심각도 수준이 `LOGGER_SEVERITY_DEFAULT`보다 낮으면 제어가 실패합니다.

DMS에서는 마이그레이션 프로세스 중에 Amazon CloudWatch를 사용하여 정보를 로그합니다. 로깅 작업 설정을 사용하면 기록할 구성 요소 활동과 기록할 정보의 양을 지정할 수 있습니다. 다음 작업에 대한 로깅을 지정해야 합니다.

- `SOURCE_CAPTURE` - 진행 중인 복제 또는 변경 데이터 캡처(CDC) 데이터는 소스 데이터베이스 또는 서비스에서 캡처되어 `SORTER` 서비스 구성 요소로 전달됩니다.
- `SOURCE_UNLOAD` - 전체 로드 중에 소스 데이터베이스 또는 서비스에서 데이터가 언로드됩니다.

로깅은 모니터링, 문제 해결, 감사, 성능 분석, 오류 탐지, 복구, 기간별 분석 및 보고를 가능하게 함으로써 DMS 복제 작업에서 중요한 역할을 합니다. 이를 통해 데이터 무결성을 유지하고 규제 요구 사항을 준수하면서 데이터베이스 간에 데이터를 성공적으로 복제할 수 있습니다. 문제 해결 중에 이러

한 구성 요소에는 DEFAULT 이외의 로깅 수준이 거의 필요하지 않습니다. 지원에서 특별히 변경을 요청하지 않는 한 이러한 구성 요소에 대한 로깅 수준을 DEFAULT으로 유지하는 것이 좋습니다. 최소 로깅 수준 DEFAULT을 사용하면 정보 메시지, 경고 및 오류 메시지가 로그에 기록됩니다. 이 제어는 이전 복제 작업에 대한 로깅 수준이 LOGGER_SEVERITY_DEFAULT, LOGGER_SEVERITY_DEBUG 또는 LOGGER_SEVERITY_DETAILED_DEBUG 중 하나 이상인지 확인합니다.

문제 해결

소스 데이터베이스 DMS 복제 작업에 대한 로깅을 활성화하려면 AWS Database Migration Service사용 설명서의 AWS DMS작업 로그 보기 및 관리를 참조하세요.

[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: AWS::DMS::Endpoint

AWS Config 규칙: dms-endpoint-ssl-configured

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS DMS엔드포인트가 SSL 연결을 사용하는지 여부를 확인합니다. 엔드포인트가 SSL을 사용하지 않으면 제어가 실패합니다.

SSL/TLS 연결은 DMS 복제 인스턴스와 데이터베이스 간의 연결을 암호화하여 보안 계층을 제공합니다. 인증서를 사용하면 예상 데이터베이스에 연결 중인지 확인하여 추가 보안 계층을 제공합니다. 프로비저닝하는 모든 데이터베이스 인스턴스에 자동으로 설치되는 서버 인증서를 확인하여 이를 수행합니다. DMS 엔드포인트에서 SSL 연결을 활성화하면 마이그레이션 중에 데이터의 기밀을 보호할 수 있습니다.

문제 해결

새로운 DMS 엔드포인트 또는 기존 DMS 엔드포인트에 SSL 연결을 추가하려면 AWS Database Migration Service 사용 설명서의 AWS Database Migration Service와 함께 SSL 사용을 참조하세요.

[DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::DMS::Endpoint`

AWS Config 규칙: dms-neptune-iam-authorization-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Neptune 데이터베이스의 AWS DMS엔드포인트가 IAM 권한 부여로 구성되어 있는지 확인합니다. DMS 엔드포인트에 IAM 권한 부여가 활성화되지 않은 경우, 제어가 실패합니다.

AWS Identity and Access Management(IAM)는 전체적으로 세분화된 액세스 제어를 제공합니다AWS. IAM을 사용하면 어떤 서비스 및 리소스에 액세스할 수 있는 사용자와 어떤 조건에서 액세스할 수 있는지 지정할 수 있습니다. IAM 정책을 사용하면 직원 및 시스템에 대한 권한을 관리하여 최소 권한 권한을 보장할 수 있습니다. Neptune 데이터베이스의 AWS DMS엔드포인트에서 IAM 권한 부여를 활성화하면 `ServiceAccessRoleARN` 파라미터에 지정된 서비스 역할을 사용하여 IAM 사용자에게 권한 부여 권한을 부여할 수 있습니다.

문제 해결

Neptune 데이터베이스에 대한 DMS 엔드포인트에서 IAM 인증을 활성화하려면 AWS Database Migration Service 사용 설명서의 AWS Database Migration Service의 대상으로 Amazon Neptune 사용을 참조하세요.

[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::DMS::Endpoint`

AWS Config 규칙: dms-mongo-db-authentication-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 MongoDB의 AWS DMS엔드포인트가 인증 메커니즘으로 구성되어 있는지 확인합니다. 엔드포인트에 인증 유형이 설정되지 않은 경우, 제어가 실패합니다.

AWS Database Migration Service는 MongoDB 버전 2.x용 MONGODB-CR과 MongoDB 버전 3.x 이상용 SCRAM-SHA-1이라는 두 가지 MongoDB 인증 방법을 지원합니다. 이러한 인증 방법은 사용자가 암호를 사용하여 데이터베이스에 액세스하려는 경우, MongoDB 암호를 인증하고 암호화하는 데 사용됩니다. AWS DMS엔드포인트에 대한 인증은 권한이 있는 사용자만 데이터베이스 간에 마이그레이션되는 데이터에 액세스하고 수정할 수 있도록 합니다. 적절한 인증이 없으면 권한이 없는 사용자가 마이그레이션 프로세스 중에 민감한 데이터에 액세스할 수 있습니다. 이로 인해 데이터 침해, 데이터 손실 또는 기타 보안 사고가 발생할 수 있습니다.

문제 해결

MongoDB DMS 엔드포인트에서 인증 메커니즘을 활성화하려면 AWS Database Migration Service 사용 설명서의 AWS DMS의 소스로 MongoDB 사용을 참조하세요.

[DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13, PCI DSS v4.0.1/4.2.1

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::DMS::Endpoint`

AWS Config 규칙: dms-redis-tls-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Redis OSS의 AWS DMS엔드포인트가 TLS 연결로 구성되어 있는지 확인합니다. 엔드포인트에 TLS가 활성화되지 않은 경우, 제어가 실패합니다.

TLS는 인터넷을 통해 애플리케이션 또는 데이터베이스 간에 데이터를 전송할 때 엔드 투 엔드 보안을 제공합니다. DMS 엔드포인트에 대한 SSL 암호화를 구성하면 마이그레이션 프로세스 중에 소스와 대상 데이터베이스 간의 암호화된 통신이 활성화됩니다. 이렇게 하면 악의적인 공격자가 민감한 데이터를 도청하고 가로채는 것을 방지할 수 있습니다. SSL 암호화가 없으면 민감한 데이터에 액세스하여 데이터 침해, 데이터 손실 또는 기타 보안 인시던트가 발생할 수 있습니다.

문제 해결

Redis용 DMS 엔드포인트에서 TLS 연결을 활성화하려면 AWS Database Migration Service 사용 설명서의 AWS Database Migration Service의 대상으로 Redis 사용을 참조하세요.

[DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::DMS::ReplicationInstance`

AWS Config 규칙: dms-replication-instance-multi-az-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Database Migration Service(AWS DMS) 복제 인스턴스가 여러 가용 영역을 사용하도록 구성되어 있는지 확인합니다(다중 AZ 배포). AWS DMS 복제 인스턴스가 다중 AZ 배포를 사용하도록 구성되지 않은 경우 제어가 실패합니다.

다중 AZ 배포에서는 다른 가용 영역(AZ)에 복제 인스턴스의 대기 복제본을 AWS DMS자동으로 프로비저닝하고 유지 관리합니다. 그러면 기본 복제 인스턴스가 대기 복제본에 동기식으로 복제됩니다. 기본 복제 인스턴스에 장애가 발생하거나 무응답 상태가 되면 대기 복제본은 중단을 최소화하면서 실행 중이던 작업을 다시 시작합니다. 자세한 내용은 AWS Database Migration Service 사용 설명서의 복제 인스턴스 작업을 참조하세요.

문제 해결

AWS DMS복제 인스턴스를 생성한 후 해당 인스턴스에 대한 다중 AZ 배포 설정을 변경할 수 있습니다. 기존 복제 인스턴스의 이 설정 및 기타 설정을 변경하는 방법에 대한 자세한 내용은 AWS Database Migration Service 사용 설명서의 복제 인스턴스 수정을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS DataSync

이러한 Security Hub CSPM 제어는 AWS DataSync서비스와 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::DataSync::Task`

AWS Config 규칙: datasync-task-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS DataSync작업에 로깅이 활성화되어 있는지 확인합니다. 작업에 로깅이 활성화되어 있지 않으면 제어가 실패합니다.

감사 로그는 시스템 활동을 추적하고 모니터링합니다. 보안 침해를 감지하고, 사고를 조사하고, 규정을 준수하는 데 도움이 되는 이벤트 기록을 제공합니다. 또한 감사 로그는 조직의 전반적인 책임과 투명성을 향상시킵니다.

문제 해결

AWS DataSync작업에 대한 로깅 구성에 대한 자세한 내용은 AWS DataSync사용 설명서의 Amazon CloudWatch Logs를 사용하여 데이터 전송 모니터링을 참조하세요.

[DataSync.2] DataSync 태스크에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::DataSync::Task`

AWS Config 규칙: datasync-task-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS DataSync작업에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 태스크에게 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 태스크에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS DataSync작업에 태그를 추가하는 방법에 대한 자세한 내용은 AWS DataSync사용 설명서의 AWS DataSync작업 태그 지정을 참조하세요.

## Amazon Detective에 대한 Security Hub CSPM 제어

이 AWS Security Hub CSPM제어는 Amazon Detective 서비스 및 리소스를 평가합니다. 일부 AWS 리전에서는 이 제어를 사용하지 못할 수도 있습니다. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Detective::Graph`

AWS Config규칙: `tagged-detective-graph` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon Detective 동작 그래프에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 동작 그래프에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 동작 그래프에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태

그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Detective 동작 그래프에 태그를 추가하려면 Amazon Detective 관리 안내서의 동작 그래프에 태그 추가를 참조하세요.

## Amazon DocumentDB에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon DocumentDB(MongoDB 호환) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: docdb-cluster-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DocumentDB 클러스터가 저장 시 암호화되는지 확인합니다. Amazon DocumentDB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 이러한 데이터의 기밀을 보호하여 권한이 없는 사용자가 데이터에 액세스할 위험을 줄일 수 있습니다. Amazon DocumentDB 클러스터의 데이터는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다. Amazon DocumentDB는 256비트 고급 암호화 표준(AES-256)을 사용하여 AWS Key Management Service(AWS KMS)에 저장된 암호화 키를 사용하여 데이터를 암호화합니다.

문제 해결

Amazon DocumentDB 클러스터를 생성할 때 저장 시 암호화를 활성화할 수 있습니다. 클러스터를 생성한 후에는 암호화 설정을 변경할 수 없습니다. 자세한 내용은 Amazon DocumentDB 개발자 안내서의 Amazon DocumentDB 클러스터에 대한 저장 시 암호화 활성화를 참조하세요.

[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-12, PCI DSS v4.0.1/3.2.1

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: docdb-cluster-backup-retention-check

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `minimumBackupRetentionPeriod` | 백업 보존 기간(일수) | Integer | 7~35 | 7 | |

이 제어는 Amazon DocumentDB 클러스터의 백업 보존 기간이 지정된 기간 이상인지 여부를 확인합니다. 백업 보존 기간이 지정된 기간 미만인 경우, 제어가 실패합니다. 백업 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구하고 시스템의 복원력을 강화할 수 있습니다. Amazon DocumentDB 클러스터의 백업을 자동화하면 시스템을 특정 시점으로 복원하고 가동 중지 시간과 데이터 손실을 최소화할 수 있습니다. Amazon DocumentDB에서 클러스터의 기본 백업 보존 기간은 1일입니다. 이 제어를 통과하려면 이 값을 7일에서 35일 사이의 값으로 늘려야 합니다.

문제 해결

Amazon DocumentDB 클러스터의 백업 보존 기간을 변경하려면 Amazon DocumentDB 개발자 안내서의 Amazon DocumentDB 클러스터 수정을 참조하세요. 백업에서 백업 보존 기간을 선택합니다.

[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::RDS::DBClusterSnapshot`

AWS Config 규칙: docdb-cluster-snapshot-public-prohibited

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DocumentDB 수동 클러스터 스냅샷이 퍼블릭인지 여부를 확인합니다. 수동 클러스터 스냅샷이 퍼블릭인 경우, 제어가 실패합니다.

Amazon DocumentDB 수동 클러스터 스냅샷은 의도한 경우가 아니면 공개해서는 안 됩니다. 암호화되지 않은 수동 스냅샷을 공개로 공유하면 모든 AWS 계정에서 해당 스냅샷을 사용할 수 있습니다. 퍼블릭 스냅샷은 의도하지 않은 데이터 노출을 초래할 수 있습니다.

> **Note**
>
> 이 제어는 수동 클러스터 스냅샷을 평가합니다. Amazon DocumentDB 자동 클러스터 스냅샷은 공유할 수 없습니다. 그러나 자동 스냅샷을 복사하여 수동 스냅샷을 생성한 다음 복사본을 공유할 수 있습니다.

문제 해결

Amazon DocumentDB 수동 클러스터 스냅샷에 대한 퍼블릭 액세스를 제거하려면 Amazon DocumentDB 개발자 안내서의 스냅샷 공유를 참조하세요. 프로그래밍 방식으로 Amazon DocumentDB 작업 `modify-db-snapshot-attribute`을 사용할 수 있습니다. `attribute-name`를 `restore`으로 설정하고 `values-to-remove`을 `all`로 설정합니다.

[DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: docdb-cluster-audit-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DocumentDB 클러스터가 Amazon CloudWatch Logs에 감사 로그를 게시하는지 여부를 확인합니다. 클러스터가 감사 로그를 CloudWatch Logs에 게시하지 않으면 제어가 실패합니다.

Amazon DocumentDB(MongoDB 호환)를 사용하면 클러스터에서 수행된 이벤트를 감사할 수 있습니다. 기록되는 이벤트의 예제로는 성공 또는 실패한 인증 시도, 데이터베이스에서 모음 삭제 또는 인덱스 생성이 있습니다. Amazon DocumentDB에서는 기본적으로 감사가 비활성화되어 있으므로 이를 활성화하려면 조치를 취해야 합니다.

문제 해결

Amazon DocumentDB 감사 로그를 CloudWatch Logs에 게시하려면 Amazon DocumentDB 개발자 안내서의 감사 활성화를 참조하세요.

[DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: docdb-cluster-deletion-protection-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DocumentDB 클러스터의 삭제 방지 기능 활성화 여부를 확인합니다. 클러스터에 삭제 방지 기능이 활성화되지 않은 경우, 제어가 실패합니다.

클러스터 삭제 방지를 활성화하면 우발적인 데이터베이스 삭제 또는 권한 없는 사용자에 의한 삭제에 대한 추가 보호 계층이 제공됩니다. 삭제 방지가 활성화되어 있는 동안에는 Amazon DocumentDB 클러스터가 삭제될 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 방지를 비활성화해야 합니다. Amazon DocumentDB 콘솔에서 클러스터를 생성하면 삭제 방지 기능이 기본적으로 활성화됩니다.

문제 해결

기존 Amazon DocumentDB 클러스터에 대한 삭제 방지를 활성화하려면 Amazon DocumentDB 개발자 안내서의 Amazon DocumentDB 클러스터 수정을 참조하세요. 클러스터 수정 섹션에서 삭제 방지 활성화를 선택합니다.

[DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: docdb-cluster-encrypted-in-transit

스케줄 유형: 주기적

파라미터: `excludeTlsParameters`: `disabled`, `enabled`(사용자 지정할 수 없음)

이 제어는 Amazon DocumentDB 클러스터가 클러스터 연결에 TLS를 요구하는지 여부를 확인합니다. 클러스터와 연결된 클러스터 파라미터 그룹이 동기화되지 않았거나 TLS 클러스터 파라미터가 `disabled` 또는 `enabled`로 설정된 경우 제어가 실패합니다.

TLS를 사용하여 애플리케이션과 Amazon DocumentDB 클러스터 간의 연결을 암호화할 수 있습니다. TLS를 사용하면 애플리케이션과 Amazon DocumentDB 클러스터 간에 데이터가 전송되는 동안 데이터가 가로채어지지 않도록 보호할 수 있습니다. Amazon DocumentDB 클러스터의 전송 중 암호화는 클러스터와 연결된 클러스터 파라미터 그룹의 TLS 파라미터를 통해 관리됩니다. 전송 중 데이터 암호화가 활성화된 경우 클러스터에 연결하려면 TLS를 사용하는 보안 연결이 필요합니다. 다음 시나리오에 TLS 파라미터 `tls1.2+`, `tls1.3+` 및 `fips-140-3`을 사용하는 것이 좋습니다.

문제 해결

Amazon DocumentDB 클러스터의 TLS 설정을 변경하는 방법에 대한 자세한 내용은 Amazon DocumentDB 개발자 안내서의 전송 중 데이터 암호화를 참조하세요.

## DynamoDB에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon DynamoDB 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[DynamoDB.1] DynamoDB 테이블은 수요에 따라 용량을 자동으로 확장해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: `dynamodb-autoscaling-enabled`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 유효한 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `minProvisionedReadCapacity` | DynamoDB Auto Scaling에 프로비저닝된 최소 읽기 용량 유닛 수 | Integer | `1~40000` | 기본값 없음 |
| `targetReadUtilization` | 읽기 용량의 목표 사용률(%) | Integer | `20~90` | 기본값 없음 |
| `minProvisionedWriteCapacity` | DynamoDB Auto Scaling에 프로비저닝된 최소 쓰기 용량 유닛 수 | Integer | `1~40000` | 기본값 없음 |
| `targetWriteUtilization` | 쓰기 용량의 목표 사용률(%) | Integer | `20~90` | 기본값 없음 |

이 제어는 Amazon DynamoDB 테이블이 필요에 따라 읽기 및 쓰기 용량을 확장할 수 있는지 여부를 확인합니다. 테이블이 온디맨드 용량 모드 또는 Auto Scaling이 구성된 프로비저닝 모드를 사용하는 경우, 이 제어가 실패합니다. 기본적으로 이 제어는 특정 수준의 읽기 또는 쓰기 용량에 관계없이 이러한 모드 중 하나만 구성하면 됩니다. 필요에 따라 특정 수준의 읽기 및 쓰기 용량 또는 목표 사용률을 요구하는 사용자 지정 파라미터 값을 제공할 수 있습니다.

수요에 따라 용량을 확장하면 제한 예외를 방지하여 애플리케이션의 가용성을 유지하는 데 도움이 됩니다. 온디맨드 용량 모드의 DynamoDB 테이블은 DynamoDB 처리량 기본 테이블 할당량에 의해서만 제한됩니다. 이러한 할당량을 늘리려면 지원 티켓을 제출할 수 있습니다지원. Auto Scaling을 사용하는 프로비저닝 모드의 DynamoDB 테이블은 트래픽 패턴에 따라 프로비저닝된 처리량 용량을 동적으로 조정합니다. DynamoDB 요청 제한에 대한 자세한 내용은 Amazon DynamoDB 개발자 안내서의 요청 제한 및 버스트 용량을 참조하세요.

문제 해결

용량 모드에서 기존 테이블에 대해 DynamoDB Auto Scaling을 활성화하려면 Amazon DynamoDB 개발자 안내서의 기존 테이블에 대한 DynamoDB Auto Scaling 활성화를 참조하세요.

[DynamoDB.2] DynamoDB 테이블에는 시점 복구가 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config 규칙: `dynamodb-pitr-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DynamoDB 테이블에 대해 PITR(시점 복구)이 활성화되어 있는지 확인합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있습니다. 또한 시스템의 복원력을 강화합니다. DynamoDB 시점 복구는 DynamoDB 테이블에 대한 백업을 자동화합니다. 이는 실수로 인한 삭제 또는 쓰기 작업을 복구하는 데 걸리는 시간을 줄여줍니다. PITR이 활성화된 DynamoDB 테이블은 최근 35일 중 원하는 시점으로 복원할 수 있습니다.

문제 해결

DynamoDB 테이블을 특정 시점으로 복원하려면 Amazon DynamoDB 개발자 안내서의 DynamoDB 테이블을 특정 시점으로 복원을 참조하세요.

[DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::DAX::Cluster`

AWS Config 규칙: `dax-encryption-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon DynamoDB Accelerator(DAX) 클러스터의 저장 시 암호화 여부를 확인합니다. DAX 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터를 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다AWS. 암호화는 권한이 없는 사용자가 데이터에 액세스하는 능력을 제한하기 위해 또 다른 액세스 제어 세트를 추가합니다. 예를 들어, 데이터를 읽기 전에 해독하려면 API 권한이 필요합니다.

문제 해결

클러스터가 생성된 후에는 저장 시 암호화를 활성화하거나 비활성화할 수 없습니다. 저장 시 암호화를 활성화하려면 클러스터를 다시 생성해야 합니다. 저장 시 암호화가 활성화된 DAX 클러스터를 생성하는 방법에 대한 자세한 지침은 Amazon DynamoDB 개발자 안내서의 AWS Management Console를 사용하여 저장 시 암호화 활성화를 참조하세요.

[DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config규칙: `dynamodb-resources-protected-by-backup-plan`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `backupVaultLockCheck` | 파라미터가 로 설정되어 `true` 있고 리소스가 AWS Backup볼트 잠금을 사용하는 경우 제어가 `PASSED` 결과를 생성합니다. | 부울 | `true` 또는 `false` | 기본값 없음 |

이 제어는 ACTIVE 상태의 Amazon DynamoDB 테이블이 백업 계획에 포함되는지 여부를 평가합니다. DynamoDB 테이블이 백업 계획에 포함되지 않는 경우, 제어가 실패합니다. backupVaultLockCheck 파라미터를와 동일하게 설정하면 DynamoDB 테이블이 AWS Backup잠긴 볼트에 백업된 경우에만 true제어가 전달됩니다.

AWS Backup는에서 데이터 백업을 중앙 집중화하고 자동화하는 데 도움이 되는 완전 관리형 백업 서비스입니다AWS 서비스. 를 사용하면 데이터 백업 빈도 및 백업 보존 기간과 같은 백업 요구 사항을 정의하는 백업 계획을 생성할 AWS Backup수 있습니다. 백업 계획에 DynamoDB 테이블을 포함하면 의도하지 않은 손실이나 삭제로부터 데이터를 보호할 수 있습니다.

문제 해결

AWS Backup백업 계획에 DynamoDB 테이블을 추가하려면 AWS Backup개발자 안내서의 백업 계획에 리소스 할당을 참조하세요.

[DynamoDB.5] DynamoDB 테이블에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: AWS::DynamoDB::Table

AWS Config규칙: tagged-dynamodb-table (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| requiredTagKeys | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | No default value |

이 제어는 Amazon DynamoDB 테이블에 파라미터 requiredTagKeys에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 테이블에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가

없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 테이블에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

DynamoDB 테이블에 태그를 추가하려면 Amazon DynamoDB 개발자 안내서의 DynamoDB에서 리소스 태깅을 참조하세요.

[DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 중간

리소스 유형: `AWS::DynamoDB::Table`

AWS Config규칙: `dynamodb-table-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon DynamoDB 테이블의 삭제 방지 기능 활성화 여부를 확인합니다. DynamoDB 테이블에 삭제 방지 기능이 활성화되지 않은 경우, 제어가 실패합니다.

삭제 보호 속성을 사용하여 DynamoDB 테이블이 실수로 삭제되지 않도록 보호할 수 있습니다. 테이블에 이 속성을 활성화하면 관리자가 일반적인 테이블 관리 작업을 수행하는 동안 테이블이 실수로 삭제되는 것을 방지할 수 있습니다. 이렇게 하면 정상적인 비즈니스 운영이 중단되는 것을 방지하는 데 도움이 됩니다.

문제 해결

DynamoDB 테이블에 대한 삭제 보호를 활성화하려면 Amazon DynamoDB 개발자 안내서의 삭제 보호 사용을 참조하세요.

[DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::DAX::Cluster`

AWS Config 규칙: `dax-tls-endpoint-encryption`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 엔드포인트 암호화 유형을 TLS로 설정하여 Amazon DynamoDB Accelerator(DAX) 클러스터가 전송 중에 암호화되는지 여부를 확인합니다. DAX 클러스터가 전송 중에 암호화되지 않으면 제어가 실패합니다.

HTTPS(TLS)를 사용하여 잠재적 공격자가 중간자 또는 그와 유사한 공격을 사용하여 네트워크 트래픽을 염탐하거나 조작하지 못하게 할 수 있습니다. DAX 클러스터에 액세스하려면 TLS를 통한 암호화된 연결만 허용해야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다.

문제 해결

DAX 클러스터를 생성한 후에는 TLS 암호화 설정을 변경할 수 없습니다. 기존 DAX 클러스터를 암호화하려면 전송 중 암호화를 활성화한 새로운 클러스터를 생성하고 애플리케이션의 트래픽을 해당 클러

스터로 이동한 다음 이전 클러스터를 삭제합니다. 자세한 내용은 Amazon DynamoDB 개발자 안내서의 삭제 보호 기능 사용을 참조하세요.

## Amazon EC2에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon Elastic Compute Cloud(Amazon EC2) 서비스 및 리소스를 평가합니다. 제어 기능을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[EC2.1] Amazon EBS 스냅샷은 공개적으로 복원 가능하도록 구성해서는 안 됩니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `ebs-snapshot-public-restorable-check`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Elastic Block Store 스냅샷이 공개적으로 복원 가능하도록 구성되어 있는지 확인합니다. Amazon EBS 스냅샷이 모두 복원 가능하도록 구성된 경우 제어가 실패합니다.

EBS 스냅샷은 특정 시점에 EBS 볼륨의 데이터를 Amazon S3에 백업하는 데 사용됩니다. 스냅샷을 사용하여 EBS 볼륨의 이전 상태를 복원할 수 있습니다. 스냅샷을 퍼블릭과 공유하는 것은 거의 허용되지 않습니다. 일반적으로 스냅샷을 공개적으로 공유하기로 결정한 것은 오류이거나 그 의미를 완전히 이해하지 못한 채 이루어졌습니다. 이 확인을 통해 이러한 모든 공유가 완전히 계획되고 의도적으로 이루어졌는지 확인할 수 있습니다.

문제 해결

퍼블릭 EBS 스냅샷을 프라이빗으로 만들려면 Amazon EC2 사용 설명서의 스냅샷 공유를 참조하세요. 작업, 권한 수정에서 비공개를 선택합니다.

[EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 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, CIS AWS 파운데이션 벤치마크 v1.2.0/4.3, CIS AWS 파운데이션 벤치마크 v1.4.0/5.3, CIS AWS 파운데이션 벤치마크 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, NIST.001 NIST.800-53.r5 SC-7

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `vpc-default-security-group-closed`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 VPC의 기본 보안 그룹이 인바운드 또는 아웃바운드 트래픽을 허용하는지 여부를 확인합니다. 보안 그룹이 인바운드 또는 아웃바운드 트래픽을 허용하는 경우, 제어가 실패합니다.

기본 보안 그룹의 규칙은 동일한 보안 그룹에 할당된 네트워크 인터페이스(및 연결된 인스턴스)로부터의 모든 아웃바운드 및 인바운드 트래픽을 허용합니다. 기본 보안 정책을 사용하지 않는 것이 좋습니다. 기본 보안 그룹은 삭제할 수 없으므로 기본 보안 그룹 규칙 설정을 변경하여 인바운드 및 아웃바운드 트래픽을 제한해야 합니다. 이렇게 하면 EC2 인스턴스와 같은 리소스에 대해 기본 보안 그룹이 실수로 구성된 경우, 의도하지 않은 트래픽을 방지할 수 있습니다.

문제 해결

이 문제를 해결하려면 먼저 최소 권한의 보안 그룹을 새로 만들어야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 생성을 참조하세요. 그런 다음 새로운 보안 그룹을 EC2 인스턴스에 할당합니다. 지침은 Amazon EC2 사용 설명서의 인스턴스의 보안 그룹 변경을 참조하세요.

새로운 보안 그룹을 리소스에 할당한 후 기본 보안 그룹에서 모든 인바운드 및 아웃바운드 규칙을 제거합니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 규칙 구성을 참조하세요.

[EC2.3] 연결된 Amazon EBS 볼륨은 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EC2::Volume`

AWS Config 규칙: `encrypted-volumes`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 연결 상태인 EBS 볼륨이 암호화되었는지 확인합니다. 이 확인을 통과하려면 EBS 볼륨이 사용 중이고 암호화되어야 합니다. EBS 볼륨이 연결되어 있지 않으면 이 확인 범위에 속하지 않습니다.

EBS 볼륨에서 중요한 데이터의 보안을 강화하려면 유휴 상태에서 EBS 암호화를 활성화해야 합니다. Amazon EBS 암호화는 자체 키 관리 인프라를 사용자가 직접 구축, 유지 및 보호할 필요가 없는 EBS 리소스에 대한 간단한 암호화 솔루션을 제공합니다. 암호화된 볼륨과 스냅샷을 생성할 때 KMS 키를 사용합니다.

Amazon EBS 암호화에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EBS 암호화를 참조하세요.

이제 Security Hub가 와 통합되었습니다

기존의 암호화되지 않은 볼륨 또는 스냅샷을 암호화하는 직접적인 방법은 없습니다. 새로운 볼륨이나 스냅샷을 생성할 때만 암호화할 수 있습니다.

암호화를 기본적으로 활성화한 경우, Amazon EBS는 Amazon EBS 암호화에 대한 사용자의 기본 키를 사용하여, 결과로 얻은 새로운 볼륨 또는 스냅샷을 암호화합니다. 암호화를 기본적으로 활성화하지 않은 경우라도 개별 볼륨 또는 스냅샷을 생성할 때 암호화를 활성화할 수 있습니다. 두 경우 모두 Amazon EBS 암호화의 기본 키를 재정의하고 대칭 고객 관리형 키를 선택할 수 있습니다.

자세한 내용은 Amazon EC2 사용 설명서의 Amazon EBS 볼륨 생성 및 Amazon EBS 스냅샷 복사를 참조하세요.

[EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리

심각도: 중간

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-stopped-instance-days-check` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `AllowedDays` | 조사 결과 실패를 생성하기 전에 EC2 인스턴스를 중지된 상태로 둘 수 있는 기간(일수) | Integer | `1~365` | `30` |

이 제어는 Amazon EC2 인스턴스가 허용된 일수보다 오랫동안 중지되어 있는지 확인합니다. EC2 인스턴스가 최대 허용 기간보다 오랫동안 중지되면 제어가 실패합니다. 허용되는 최대 기간 동안 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 30일을 사용합니다.

EC2 인스턴스를 상당 기간 실행하지 않으면 인스턴스가 활발하게 유지 관리(분석, 패치, 업데이트)되지 않아 보안 위험이 발생합니다. 나중에 시작하면 적절한 유지 관리가 부족하여 AWS 환경에서 예기치 않은 문제가 발생할 수 있습니다. 일정 기간 동안 EC2 인스턴스를 비활성 상태로 안전하게 유지 관리하려면 유지 관리를 위해 주기적으로 시작한 다음 유지 관리 후에 중지하세요. 이 프로세스는 자동화된 것이 이상적입니다.

> **Note**
>
> 이 제어는 인스턴스에 대해의 타임스탬프를 사용하여 EC2 인스턴스가 중지된 일수`StateTransitionReason`를 평가합니다. 에 타임스탬프가 포함되지 `StateTransitionReason` 않은 경우(예: 내부 오류로 인해 인스턴스가 중지된 경우) 제어는 인스턴스의 시작 시간을 대신 사용합니다. 이 경우 시작 시간이 최대 허용 기간보다 오래된 경우 제어는 FAILED 결과를 생성합니다.

문제 해결

EC2 인스턴스 종료에 대한 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 종료를 참조하세요.

[EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/3.7, CIS AWS 파운데이션 벤치마크 v1.2.0/2.9, CIS AWS 파운데이션 벤치마크 v1.4.0/3.9, CIS AWS 파운데이션 벤치마크 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-3, NIST.800-53.r5 AU-6(3), NIST.800-53.r5 AU-6(4), NIST.800-53.r5 CA-7 SI-7 3.1.2010.3.310.3.410.3.510.3.6

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::EC2::VPC`

AWS Config 규칙: `vpc-flow-logs-enabled`

스케줄 유형: 주기적

파라미터:

- `trafficType`: `REJECT`(사용자 지정할 수 없음)

이 제어는 Amazon VPC 흐름 로그가 발견되어 VPC에 대해 활성화되어 있는지 확인합니다. 트래픽 유형이 `Reject`로 설정되어 있습니다. 계정의 VPC에 대해 VPC 흐름 로그를 활성화하지 않으면 제어가 실패합니다.

> **Note**
>
> 이 제어는 AWS 계정에 대해 Amazon Security Lake를 통해 Amazon VPC 흐름 로그가 활성화되었는지 여부를 확인하지 않습니다.

VPC 흐름 로그 기능을 사용하면 VPC의 네트워크 인터페이스에서 들어오고 나가는 IP 주소 트래픽에 대한 정보를 캡처할 수 있습니다. 흐름 로그를 생성한 후 CloudWatch Logs에서 해당 데이터를 보고 검색할 수 있습니다. 비용을 줄이기 위해 Amazon S3로 흐름 로그를 전송할 수도 있습니다.

Security Hub CSPM은 VPCs의 패킷 거부에 대해 흐름 로깅을 활성화할 것을 권장합니다. 흐름 로그는 VPC를 통과하는 네트워크 트래픽에 대한 가시성을 제공하고 비정상적인 트래픽을 감지하거나 보안 워크플로 중에 인사이트를 제공할 수 있습니다.

기본적으로 레코드에는 소스, 대상 및 프로토콜을 포함하여 IP 주소 흐름의 다른 구성 요소에 대한 값이 포함됩니다. 로그 필드에 대한 자세한 내용 및 설명은 Amazon VPC 사용 설명서의 VPC 흐름 로그를 참조하세요.

문제 해결

VPC 흐름 로그를 생성하려면 Amazon VPC 사용 설명서의 흐름 로그 생성을 참조하세요. Amazon VPC 콘솔을 연 다음 VPC를 선택합니다. 필터에서 거부 또는 전부를 선택합니다.

[EC2.7] EBS 기본 암호화를 활성화해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/5.1.1, CIS AWS 파운데이션 벤치마크 v1.4.0/2.2.1, CIS AWS 파운데이션 벤치마크 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `ec2-ebs-encryption-by-default`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 계정 수준 암호화가 기본적으로 활성화되어 있는지 확인합니다. EBS 볼륨에 계정 수준 암호화가 활성화되지 않은 경우 제어가 실패합니다.

계정에 암호화가 활성화되면 Amazon EBS 볼륨과 스냅샷 사본이 저장 중 암호화됩니다. 그러면 데이터 보호 계층이 하나 더 추가됩니다. 자세한 내용은 Amazon EC2 사용 설명서에서 기본적으로 암호화를 참조하세요.

문제 해결

Amazon EBS 볼륨에 대한 기본 암호화를 구성하려면 Amazon EC2 사용 설명서의 기본 암호화를 참조하세요.

[EC2.8] EC2 인스턴스는 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/5.7, CIS AWS 파운데이션 벤치마크 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

범주: 보호 > 네트워크 보안

심각도: 높음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-imdsv2-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 인스턴스 메타데이터 버전이 IMDSv2(인스턴스 메타데이터 서비스 버전 2)로 구성되어 있는지 확인합니다. IMDSv2에 대해 `HttpTokens`이 필수로 설정된 경우, 제어가 통과됩니다. `HttpTokens`을 `optional`로 설정하면 제어가 실패합니다.

인스턴스 메타데이터를 사용하여 실행 중인 인스턴스를 구성하거나 관리합니다. IMDS는 자주 교체되는 임시 보안 인증 정보에 대한 액세스를 제공합니다. 이러한 보안 인증을 사용하면 민감한 보안 인증 정보를 수동으로 또는 프로그래밍 방식으로 인스턴스에 하드 코딩하거나 배포할 필요가 없습니다. IMDS는 모든 EC2 인스턴스에 로컬로 연결됩니다. 이는 특수한 "링크 로컬" IP 주소 169.254.169.254에서 실행됩니다. 이 IP 주소는 인스턴스에서 실행되는 소프트웨어에서만 액세스할 수 있습니다.

IMDS 버전 2에는 다음 유형의 취약성에 대한 새로운 보호 기능이 추가되었습니다. 이러한 취약성을 이용하여 IMDS에 액세스할 수 있습니다.

- 개방형 웹사이트 애플리케이션 방화벽
- 개방형 리버스 프록시
- 서버 측 요청 위조(SSRF) 취약성
- 개방형 Layer 3 방화벽 및 Network Address Translation(NAT)

Security Hub CSPM은 IMDSv2로 EC2 인스턴스를 구성할 것을 권장합니다.

문제 해결

IMDSv2를 사용하여 EC2 인스턴스를 구성하려면 Amazon EC2 사용 설명서의 IMDSv2를 필요로 하는 권장 경로를 참조하세요.

[EC2.9] Amazon EC2 인스턴스에는 퍼블릭 IPv4 주소가 없어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-instance-no-public-ip`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 인스턴스에 퍼블릭 IP 주소가 있는지 여부를 확인합니다. `publicIp` 필드가 EC2 인스턴스 구성 항목에 있으면 제어가 실패합니다. 이 제어는 IPv4 주소에만 적용됩니다.

퍼블릭 IPv4 주소는 인터넷을 통해 연결할 수 있는 IP 주소입니다. 퍼블릭 IP 주소로 인스턴스를 시작하는 경우, 인터넷에서 EC2 인스턴스에 연결할 수 있습니다. 프라이빗 IPv4 주소는 인터넷을 통해 연결할 수 없는 IP 주소입니다. 동일한 VPC 또는 연결된 프라이빗 네트워크에 있는 EC2 인스턴스 간의 통신에 프라이빗 IPv4 주소를 사용할 수 있습니다.

IPv6 주소는 전역적으로 고유하므로 인터넷으로 접속할 수 있습니다. 그러나 기본적으로 모든 서브넷에는 IPv6 주소 지정 속성이 false로 설정되어 있습니다. IPv6에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPC에서 IP 주소 지정을 참조하세요.

퍼블릭 IP 주소를 사용하여 EC2 인스턴스를 유지 관리하는 합법적인 사용 사례가 있는 경우, 이 제어에서 조사 결과를 숨길 수 있습니다. 프런트엔드 아키텍처 옵션에 대한 자세한 내용은 AWS 아키텍처 블로그 또는 내 아키텍처 시리즈 AWS 비디오 시리즈를 참조하세요.

문제 해결

기본적으로 인스턴스에 퍼블릭 IP 주소가 할당되지 않도록 기본이 아닌 VPC를 사용하세요.

EC2 인스턴스를 기본 VPC로 시작하면 퍼블릭 IP 주소가 할당됩니다. 기본 VPC가 아닌 VPC에서 EC2 인스턴스를 시작하는 경우, 서브넷 구성에 따라 퍼블릭 IP 주소를 수신할지 여부가 결정됩니다. 서브넷에는 서브넷의 새로운 EC2 인스턴스가 퍼블릭 IPv4 주소 풀에서 퍼블릭 IP 주소를 수신하는지 확인하는 속성이 있습니다.

EC2 인스턴스에서 자동으로 할당된 퍼블릭 IP 주소를 수동으로 연결하거나 연결 해제할 수 없습니다. 자세한 내용은 Amazon EC2 사용 설명서의 퍼블릭 IPv4 주소 및 외부 DNS 호스트 이름을 참조하세요.

[EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > API 프라이빗 액세스

심각도: 중간

리소스 유형: `AWS::EC2::VPC`

AWS Config 규칙: vpc-endpoint-enabled

스케줄 유형: 주기적

파라미터:

- `serviceNames`: `ec2`(사용자 지정할 수 없음)

이 제어는 각 VPC에 대해 Amazon EC2용 서비스 엔드포인트가 생성되었는지 여부를 확인합니다. Amazon EC2 서비스용으로 생성된 VPC 엔드포인트가 VPC에 없으면 제어가 실패합니다.

이 제어는 단일 계정의 리소스를 평가합니다. 계정 외부에 있는 리소스는 설명할 수 없습니다. AWS Config 및 Security Hub CSPM은 교차 계정 검사를 수행하지 않으므로 계정 간에 공유되는 VPCs에 대한 `FAILED` 조사 결과를 볼 수 있습니다. Security Hub CSPM은 이러한 `FAILED` 조사 결과를 억제할 것을 권장합니다.

VPC의 보안 상태를 개선하기 위해 인터페이스 VPC 엔드포인트를 사용하도록 Amazon EC2를 구성할 수 있습니다. 인터페이스 엔드포인트는 Amazon EC2 API 작업에 비공개 AWS PrivateLink로 액세스할

수 있는 기술로 구동됩니다. 이는 VPC 및 Amazon ECR 간의 모든 네트워크 트래픽을 Amazon 네트워크로 제한합니다. 엔드포인트는 동일한 리전 내에서만 지원되므로 VPC와 다른 리전의 서비스 간에 엔드포인트를 생성할 수 없습니다. 이렇게 하면 다른 리전에 대한 의도하지 않은 Amazon EC2 API 호출을 방지할 수 있습니다.

Amazon EC2용 VPC 엔드포인트 생성에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 및 인터페이스 VPC 엔드포인트를 참조하세요.

문제 해결

Amazon VPC 콘솔에서 Amazon EC2에 대한 인터페이스 엔드포인트를 생성하려면 AWS PrivateLink 안내서의 VPC 엔드포인트 생성을 참조하세요. 서비스 이름에 com.amazonaws.***region***.ec2를 선택합니다.

또한 엔드포인트 정책을 생성하고 VPC 엔드포인트에 연결하여 Amazon EC2 API에 대한 액세스를 제어할 수도 있습니다. VPC 엔드포인트 정책 생성에 대한 지침은 Amazon EC2 사용 설명서의 엔드포인트 정책 생성을 참조하세요.

[EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다.

관련 요구 사항: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CM-8(1)

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::EC2::EIP`

AWS Config 규칙: `eip-attached`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 VPC에 할당된 탄력적 IP(EIP) 주소가 EC2 인스턴스 또는 사용 중인 탄력적 네트워크 인터페이스(ENI)에 연결되어 있는지 확인합니다.

실패한 조사 결과는 사용되지 않은 EC2 EIP가 있을 수 있음을 나타냅니다.

이는 카드 소지자 데이터 환경(CDE)에서 EIP의 정확한 자산 목록을 유지하는 데 도움이 됩니다.

문제 해결

사용하지 않은 EIP를 해제하려면 Amazon EC2 사용 설명서의 탄력적 IP 주소 해제를 참조하세요.

[EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 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), 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), NIST.800-1.r1.r1.r1.

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `restricted-ssh`

스케줄 유형: 변경이 트리거되며 주기적임

파라미터: 없음

이 제어는 Amazon EC2 보안 그룹이 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용하는지 확인합니다. 보안 그룹에서 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용하면 제어가 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 어떤 보안 그룹에서도 포트 22에 대한 무제한 수신 액세스를 허용하지 않는 것이 좋습니다. SSH와 같은 원격 콘솔 서비스에 대한 불가항력적인 연결성을 제거하면 서버가 위험에 노출될 가능성이 줄어듭니다.

문제 해결

포트 22에 대한 수신을 금지하려면 VPC와 연결된 각 보안 그룹에 대해 이러한 액세스를 허용하는 규칙을 제거하세요. 자세한 내용은 Amazon EC2 사용 설명서의 보안 그룹 규칙 업데이트를 참조하세요. Amazon EC2 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 22에 대한 액세스를 허용하는 규칙을 제거합니다.

[EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v1.2.0/4.2, PCI DSS v4.0.1/1.3.1

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `restricted-common-ports` (생성된 규칙은 `restricted-rdp`)

스케줄 유형: 변경이 트리거되며 주기적임

파라미터: 없음

이 제어는 Amazon EC2 보안 그룹이 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용하는지 확인합니다. 보안 그룹에서 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용하면 제어가 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 어떤 보안 그룹에서도 포트 3389에 대한 무제한 수신 액세스를 허용하지 않는 것이 좋습니다. RDP와 같은 원격 콘솔 서비스에 대한 불가항력적인 연결성을 제거하면 서버가 위험에 노출될 가능성이 줄어듭니다.

문제 해결

포트 3389에 대한 수신을 금지하려면 VPC와 연결된 각 보안 그룹에 대해 이러한 액세스를 허용하는 규칙을 제거하세요. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 규칙 업데이트를 참조하세요. Amazon VPC 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 3389에 대한 액세스를 허용하는 규칙을 제거합니다.

[EC2.15] Amazon EC2 서브넷은 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::EC2::Subnet`

AWS Config 규칙: `subnet-auto-assign-public-ip-disabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Virtual Private Cloud(Amazon VPC) 서브넷이 퍼블릭 IP 주소를 자동으로 할당하도록 구성되어 있는지 확인합니다. 서브넷이 퍼블릭 IPv4 또는 IPv6 주소를 자동으로 할당하도록 구성된 경우 제어가 실패합니다.

서브넷에는 네트워크 인터페이스가 퍼블릭 IPv4 및 IPv6 주소를 자동으로 수신할지 여부를 결정하는 속성이 있습니다. IPv4의 경우이 속성은 TRUE 기본 서브넷의 FALSE 경우 로 설정되고 기본이 아닌 서브넷의 경우 로 설정됩니다(EC2 인스턴스 시작 마법사를 통해 생성된 기본이 아닌 서브넷의 경우 예외, 여기서 로 설정됨TRUE). IPv6의 경우이 속성은 기본적으로 모든 서브넷에 FALSE 대해 로 설정됩니다. 이러한 속성이 활성화되면 서브넷에서 시작된 인스턴스는 기본 네트워크 인터페이스에서 해당 IP 주소(IPv4 또는 IPv6)를 자동으로 수신합니다.

문제 해결

퍼블릭 IP 주소를 할당하지 않도록 서브넷을 구성하려면 Amazon VPC 사용 설명서의 서브넷의 IP 주소 지정 속성 수정을 참조하세요.

[EC2.16] 사용하지 않는 네트워크 액세스 제어 목록은 제거해야 합니다.

관련 요구 사항: NIST.800-53.r5 CM-8(1), NIST.800-171.r2 3.4.7, PCI DSS v4.0.1/1.2.7

범주: 보호 > 네트워크 보안

심각도: 낮음

리소스 유형: `AWS::EC2::NetworkAcl`

AWS Config 규칙: `vpc-network-acl-unused-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 가상 프라이빗 클라우드(VPC)에 사용되지 않은 네트워크 액세스 제어 목록(ACL)이 있는지 확인합니다. 네트워크 ACL이 서브넷과 연결되어 있지 않으면 제어가 실패합니다. 제어는 미사용 기본 네트워크 ACL에 대한 조사 결과를 생성하지 않습니다.

제어는 리소스 `AWS::EC2::NetworkAcl`의 항목 구성을 확인하고 네트워크 ACL의 관계를 결정합니다.

유일한 관계가 네트워크 ACL의 VPC인 경우, 제어가 실패합니다.

다른 관계가 나열되면 제어가 통과합니다.

문제 해결

사용하지 않는 네트워크 ACL 삭제에 대한 지침은 Amazon VPC 사용 설명서의 네트워크 ACL 삭제를 참조하세요. 기본 네트워크 ACL 또는 서브넷에 연결된 ACL은 삭제할 수 없습니다.

[EC2.17] Amazon EC2 인스턴스는 여러 ENI를 사용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21)

범주: 보호 > 네트워크 보안

심각도: 낮음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `ec2-instance-multiple-eni-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 인스턴스가 여러 탄력적 네트워크 인터페이스(ENI) 또는 Elastic Fabric Adapter(EFA)를 사용하는지 여부를 확인합니다. 이 제어는 단일 네트워크 어댑터를 사용하는 경우, 통과됩니다. 제어에는 허용되는 ENI를 식별하기 위한 선택적 파라미터 목록이 포함되어 있습니다. Amazon EKS 클러스터에 속하는 EC2 인스턴스가 둘 이상의 ENI를 사용하는 경우에도 이 제어는 실패합니다. EC2 인스턴스에 Amazon EKS 클러스터의 일부로서 여러 ENI가 있어야 하는 경우, 이러한 제어 조사 결과를 숨길 수 있습니다.

ENI가 여러 개이면 듀얼 홈 인스턴스, 즉 서브넷이 여러 개 있는 인스턴스가 발생할 수 있습니다. 이로 인해 네트워크 보안이 복잡해지고 의도하지 않은 네트워크 경로와 액세스가 발생할 수 있습니다.

문제 해결

EC2 인스턴스에서 네트워크 인터페이스를 분리하려면 Amazon EC2 사용 설명서의 인스턴스에서 네트워크 인터페이스 분리를 참조하세요.

[EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.

관련 요구 사항: 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), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `vpc-sg-open-only-to-authorized-ports`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `authorizedTcpPorts` | 승인된 TCP 포트 목록 | IntegerList(최소 1개 항목, 최대 32개 항목) | 1~65535 | `[80,443]` |
| `authorizedUdpPorts` | 승인된 UDP 포트 목록 | IntegerList(최소 1개 항목, 최대 32개 항목) | 1~65535 | 기본값 없음 |

이 제어는 Amazon EC2 보안 그룹이 승인되지 않은 포트로부터의 무제한 수신 트래픽을 허용하는지 확인합니다. 제어 상태는 다음과 같이 결정합니다.

- `authorizedTcpPorts`의 기본값을 사용하는 경우, 보안 그룹이 포트 80 및 443 외 모든 포트로부터의 무제한 수신 트래픽을 허용하면 제어가 실패합니다.
- `authorizedTcpPorts` 또는 `authorizedUdpPorts`에 사용자 지정 값을 제공하는 경우, 보안 그룹이 목록에 없는 포트로부터의 무제한 수신 트래픽을 허용하면 제어가 실패합니다.

보안 그룹은 AWS에 대한 수신 및 송신 네트워크 트래픽의 상태 저장 필터링을 제공합니다. 보안 그룹 규칙은 최소 권한 액세스 원칙을 따라야 합니다. 무제한 액세스(접미사가 /0인 IP 주소)는 해킹, 서비스 거부 공격, 데이터 손실과 같은 악의적인 활동의 가능성을 높입니다. 포트가 특별히 허용되지 않는 한, 포트는 무제한 액세스를 거부해야 합니다.

문제 해결

보안 그룹을 수정하려면 Amazon VPC 사용 설명서에서 보안 그룹 작업을 참조하세요.

[EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.

관련 요구 사항: 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), NIST.800-53.r5 SC-7(21), NIST.800-53.r5 SC-7(4), 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

범주: 보호 > 제한된 네트워크 액세스

심각도: 심각

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `restricted-common-ports` (생성된 규칙은 `vpc-sg-restricted-common-ports`)

스케줄 유형: 변경이 트리거되며 주기적임

파라미터: `"blockedPorts": "20,21,22,23,25,110,135,143,445,1433,1434,3000,3306,3389,4333,5000,5432,5500,560` 용자 지정할 수 없음)

이 제어는 Amazon EC2 보안 그룹에 대한 무제한 수신 트래픽이 가장 위험이 높은 지정된 포트에 액세스할 수 있는지 여부를 확인합니다. 보안 그룹의 규칙 중 하나라도 '0.0.0.0/0' 또는 '::/0'에서 해당 포트로의 수신 트래픽을 허용하는 경우, 이 제어는 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 무제한 액세스(0.0.0.0/0) 때문에 악의적인 활동(해킹, 서비스 거부 공격, 데이터 손실)의 기회가 늘어납니다. 어떤 보안 그룹도 다음 포트에 대한 무제한 수신 액세스를 허용해서는 안 됩니다.

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIFS)

- 1433, 1434 (MSSQL)
- 3000 (Go, Node.js, Ruby 웹 개발 프레임워크)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (Python 웹 개발 프레임워크)
- 5432 (postgresql)
- 5500 (fcp-addr-srvr1)
- 5601 (OpenSearch 대시보드)
- 8080 (프록시)
- 8088 (레거시 HTTP 포트)
- 8888 (대체 HTTP 포트)
- 9200 또는 9300 (OpenSearch)

문제 해결

보안 그룹에서 규칙을 삭제하려면 Amazon EC2 사용 설명서의 보안 그룹에서 규칙 삭제를 참조하세요.

[EC2.20] a AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다.

관련 요구 사항: 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, NIST.800-171.r2 3.1.20

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형:`AWS::EC2::VPNConnection`

AWS Config 규칙: `vpc-vpn-2-tunnels-up`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

VPN 터널은 고객 네트워크에서 AWS Site-to-Site VPN 연결 AWS 로 또는 내에서 데이터를 전달할 수 있는 암호화된 링크입니다. 각 VPN 연결에는 고가용성을 위해 동시에 사용할 수 있는 두 개의 VPN 터

널이 포함되어 있습니다. AWS VPC와 원격 네트워크 간의 안전하고 가용성이 높은 연결을 확인하려면 두 VPN 터널이 모두 VPN 연결을 위해 준비되었는지 확인하는 것이 중요합니다.

이 제어는 AWS Site-to-Site VPN에서 제공하는 두 VPN 터널이 모두 UP 상태인지 확인합니다. 터널 중 하나 또는 두 개가 DOWN 상태인 경우, 제어가 실패합니다.

문제 해결

VPN 터널 옵션을 수정하려면Site-to-Site VPN 사용 설명서의 Site-to-Site VPN 터널 옵션 수정을 참조하세요. AWS Site-to-Site

[EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/5.2, CIS AWS 파운데이션 벤치마크 v1.4.0/5.1, CIS AWS 파운데이션 벤치마크 v3.0.0/5.1, 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(21), NIST.800-53.r5 SC-75 3.1.20

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형:`AWS::EC2::NetworkAcl`

AWS Config 규칙: `nacl-no-unrestricted-ssh-rdp`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 네트워크 액세스 제어 목록(네트워크 ACL)이 SSH/RDP 수신 트래픽의 기본 TCP 포트에 대한 무제한 액세스를 허용하는지 여부를 확인합니다. 네트워크 ACL 인바운드 항목이 TCP 포트 22 또는 3389에 대해 '0.0.0.0/0' 또는 '::/0'의 소스 CIDR 블록을 허용하는 경우, 규칙이 실패합니다. 제어는 기본 네트워크 ACL에 대한 조사 결과를 생성하지 않습니다.

포트 22(SSH) 및 포트 3389(RDP)와 같은 원격 서버 관리 포트에 대한 액세스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 VPC 내의 리소스에 의도하지 않은 액세스가 허용될 수 있습니다.

문제 해결

네트워크 ACL 트래픽 규칙을 편집하려면 Amazon VPC 사용 설명서의 네트워크 ACL 작업을 참조하세요.

[EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.

범주: 식별 > 인벤토리

심각도: 중간

리소스 유형: `AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`

AWS Config 규칙: `ec2-security-group-attached-to-eni-periodic`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 보안 그룹이 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 또는 탄력적 네트워크 인터페이스에 연결되어 있는지 확인합니다. 보안 그룹이 Amazon EC2 인스턴스 또는 탄력적 네트워크 인터페이스와 연결되어 있지 않으면 제어가 실패합니다.

> **Important**
>
> 2023년 9월 20일에 Security Hub CSPM은 AWS 기본 보안 모범 사례 및 NIST SP 800-53 개정 5 표준에서이 제어를 제거했습니다. 이 제어는 AWS Control Tower 서비스 관리형 표준의 일부입니다. 이 제어는 보안 그룹이 EC2 인스턴스 또는 탄력적 네트워크 인터페이스에 연결된 경우, 통과 조사 결과를 생성합니다. 하지만, 특정 사용 사례에 대해서는 연결되지 않은 보안 그룹이 보안 위험을 초래하지는 않습니다. EC2.2, EC2.13, EC2.14, EC2.18, EC2.19 등의 다른 EC2 제어를 사용하여 보안 그룹을 모니터링할 수 있습니다.

문제 해결

보안 그룹을 생성, 할당, 삭제하려면 Amazon EC2 사용 설명서의 EC2 인스턴스에 대한 보안 그룹을 참조하세요.

[EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21), NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형:`AWS::EC2::TransitGateway`

AWS Config 규칙: ec2-transit-gateway-auto-vpc-attach-disabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 전송 게이트웨이가 공유 VPC 연결을 자동으로 수락하는지 확인합니다. 공유된 VPC 연결 요청을 자동으로 수락하는 전송 게이트웨이에서는 이 제어가 실패합니다.

AutoAcceptSharedAttachments을 켜면 요청 또는 연결이 시작된 계정을 확인하지 않고 모든 교차 계정 VPC 연결 요청을 자동으로 수락하도록 전송 게이트웨이가 구성됩니다. 권한 부여 및 인증의 모범 사례를 따르려면 승인된 VPC 연결 요청만 허용되도록 이 기능을 끄는 것이 좋습니다.

문제 해결

전송 게이트웨이를 수정하려면 Amazon VPC 개발자 안내서의 전송 게이트웨이 수정을 참조하세요.

[EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

관련 요구 사항: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형:AWS::EC2::Instance

AWS Config 규칙: ec2-paravirtual-instance-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 EC2 인스턴스의 가상화 유형이 반가상화인지 여부를 확인합니다. EC2 인스턴스의 virtualizationType가 paravirtual로 설정된 경우, 제어가 실패합니다.

Linux Amazon Machine Image(AMI)는 PV(반가상화) 또는 HVM(하드웨어 가상 머신)의 두 가지 유형의 가상화를 사용합니다. PV AMI와 HVM AMI의 주요 차이점은 부팅 방법과 더 나은 성능을 위해 특수 하드웨어 확장(CPU, 네트워크, 스토리지)을 활용할 수 있는지 여부에 있습니다.

이전에는 대부분의 경우, PV 게스트가 HVM 게스트보다 더 나은 성능을 제공했지만, HVM 가상화 기능이 향상되고 HVM AMI용 PV 드라이버가 제공되는 현재는 더 이상 그렇지 않습니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux AMI 가상화 유형을 참조하세요.

문제 해결

EC2 인스턴스를 새로운 인스턴스 유형으로 업데이트하려면 Amazon EC2 사용 설명서의 인스턴스 유형 변경을 참조하세요.

[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형:`AWS::EC2::LaunchTemplate`

AWS Config 규칙: `ec2-launch-template-public-ip-disabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 시작 템플릿이 시작 시 네트워크 인터페이스에 퍼블릭 IP 주소를 할당하도록 구성되어 있는지 확인합니다. 네트워크 인터페이스에 퍼블릭 IP 주소를 할당하도록 EC2 시작 템플릿이 구성되어 있거나 퍼블릭 IP 주소가 있는 네트워크 인터페이스가 하나 이상 있는 경우, 제어가 실패합니다.

퍼블릭 IP 주소는 인터넷을 통해 연결할 수 있는 주소입니다. 퍼블릭 IP 주소로 네트워크 인터페이스를 구성하면 인터넷에서 해당 네트워크 인터페이스와 연결된 리소스에 연결할 수 있습니다. EC2 리소스는 워크로드에 대한 의도하지 않은 액세스를 허용할 수 있으므로 공개적으로 액세스하면 안 됩니다.

문제 해결

EC2 시작 템플릿을 업데이트하려면 Amazon EC2 Auto Scaling 사용 설명서의 기본 네트워크 인터페이스 설정 변경을 참조하세요.

[EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.

범주: 복구 > 복원력 > 백업 활성화

관련 요구 사항: 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)

심각도: 낮음

리소스 유형: `AWS::EC2::Volume`

AWS Config 규칙: `ebs-resources-protected-by-backup-plan`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `backupVaultLockCheck` | 파라미터가 `true`로 설정되어 있고 리소스가 AWS Backup Vault Lock을 사용하는 경우, 제어가 `PASSED` 조사 결과를 생성합니다. | 부울 | `true` 또는 `false` | 기본값 없음 |

이 제어는 `in-use` 상태의 Amazon EBS 볼륨이 백업 계획에 포함되는지 여부를 평가합니다. EBS 볼륨에 백업 계획이 적용되지 않는 경우, 제어가 실패합니다. `backupVaultLockCheck` 파라미터를와 동일하게 설정하면 EBS 볼륨이 AWS Backup 잠긴 볼트에 백업된 경우에만 `true`제어가 전달됩니다.

백업을 통해 보안 사고로부터 더 빨리 복구할 수 있습니다. 또한 시스템의 복원력을 강화합니다. 백업 계획에 Amazon EBS 볼륨을 포함하면 의도하지 않은 손실 또는 삭제로부터 데이터를 보호할 수 있습니다.

문제 해결

Amazon EBS 볼륨을 AWS Backup 백업 계획에 추가하려면 AWS Backup 개발자 안내서의 백업 계획에 리소스 할당을 참조하세요.

[EC2.33] EC2 Transit Gateway Attachment에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TransitGatewayAttachment`

AWS Config 규칙: `tagged-ec2-transitgatewayattachment` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 Transit Gateway Attachment에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. Transit Gateway Attachment에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 Transit Gateway Attachment 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 Transit Gateway Attachment에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TransitGatewayRouteTable`

AWS Config 규칙: `tagged-ec2-transitgatewayroutetable` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 전송 게이트웨이 라우팅 테이블이 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 전송 게이트웨이 라우팅 테이블에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 전송 게이트웨이 라우팅 테이블이 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하

는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 전송 게이트웨이 라우팅 테이블에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.35] EC2 네트워크 인터페이스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::NetworkInterface`

AWS Config 규칙: `tagged-ec2-networkinterface` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 네트워크 인터페이스에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 네트워크 인터페이스에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 네트워크 인터페이스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 네트워크 인터페이스에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.36] EC2 고객 게이트웨이에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::CustomerGateway`

AWS Config 규칙: `tagged-ec2-customergateway` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| requiredTagKeys | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 고객 게이트웨이에 파라미터 requiredTagKeys에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 고객 게이트웨이에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 고객 게이트웨이에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 고객 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅을 참조하세요.

[EC2.37] EC2 탄력적 IP 주소에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::EIP`

AWS Config 규칙: `tagged-ec2-eip` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 탄력적 IP 주소에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 탄력적 IP 주소에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 탄력전 IP 주소에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 탄력적 IP 주소에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.38] EC2 인스턴스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::Instance`

AWS Config 규칙: `tagged-ec2-instance` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 인스턴스에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 인스턴스에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 인스턴스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 인스턴스는 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅을 참조하세요.

[EC2.39] EC2 인터넷 게이트웨이에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::InternetGateway`

AWS Config 규칙: `tagged-ec2-internetgateway` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 인터넷 게이트웨이에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 인터넷 게이트웨이에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우,

제어는 태그 키의 존재만 확인하고 인터넷 게이트웨이에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 인터넷 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅을 참조하세요.

[EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::NatGateway`

AWS Config 규칙: `tagged-ec2-natgateway` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 네트워크 주소 변환(NAT) 게이트웨이에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. NAT 게이트웨이에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 NAT 게이트웨이에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 NAT 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅을 참조하세요.

[EC2.41] EC2 네트워크 ACL에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::NetworkAcl`

AWS Config 규칙: `tagged-ec2-networkacl` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 네트워크 액세스 제어 목록(네트워크 ACL)에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 네트워크 ACL에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 네트워크 ACL에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 네트워크 ACL에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.42] EC2 라우팅 테이블에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::RouteTable`

AWS Config 규칙: `tagged-ec2-routetable` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 라우팅 테이블에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 라우팅 테이블에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 라우팅 테이블에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 라우팅 테이블에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.43] EC2 보안 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `tagged-ec2-securitygroup` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon EC2 보안 그룹에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 보안 그룹에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 보안 그룹에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 보안 그룹에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅을 참조하세요.

[EC2.44] EC2 서브넷에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::Subnet`

AWS Config 규칙: `tagged-ec2-subnet` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 서브넷에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 서브넷에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 서브넷에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 서브넷에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.45] EC2 볼륨에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::Volume`

AWS Config 규칙: `tagged-ec2-volume` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 볼륨에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 볼륨에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 볼륨에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 볼륨에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.46] Amazon VPC에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPC`

AWS Config 규칙: `tagged-ec2-vpc` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Virtual Private Cloud(Amazon VPC)에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. Amazon VPC에 태그 키가 없거나 파

라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 Amazon VPC에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

VPC에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.47] Amazon VPC 엔드포인트 서비스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPCEndpointService`

AWS Config 규칙: `tagged-ec2-vpcendpointservice` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon VPC 엔드포인트 서비스에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 엔드포인트 서비스에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 엔드포인트에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

Amazon VPC 엔드포인트 서비스에 태그를 추가하려면 AWS PrivateLink 가이드의 엔드포인트 서비스 구성 섹션에서 태그 관리를 참조하세요.

[EC2.48] Amazon VPC 흐름 로그에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::FlowLog`

AWS Config 규칙: `tagged-ec2-flowlog` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon VPC 흐름 로그에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 흐름 로그에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 흐름 로그에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

Amazon VPC 흐름 로그에 태그를 추가하려면 Amazon VPC 사용 설명서의 흐름 로그 태깅을 참조하세요.

[EC2.49] Amazon VPC 피어링 연결에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPCPeeringConnection`

AWS Config 규칙: `tagged-ec2-vpcpeeringconnection` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon VPC 피어링 연결에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 피어링 연결에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 피어링 연결에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

Amazon VPC 피어링 연결에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.50] EC2 VPN 게이트웨이에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::VPNGateway`

AWS Config 규칙: `tagged-ec2-vpngateway` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 VPN 게이트웨이에 파라미터 에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. VPN 게이트웨이에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제

어는 태그 키의 존재만 확인하고 VPN 게이트웨이에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 VPN 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태깅을 참조하세요.

[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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), NIST.800-171.r2 3.1.12, NIST.800-171.r2 3.1.20, PCI DSS v4.0.1/10.2.1

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::EC2::ClientVpnEndpoint`

AWS Config 규칙: `ec2-client-vpn-connection-log-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Client VPN 엔드포인트에 클라이언트 연결 로깅이 활성화되어 있는지 확인합니다. 엔드포인트에 클라이언트 연결 로깅이 활성화되어 있지 않으면 제어가 실패합니다.

클라이언트 VPN 엔드포인트를 사용하면 원격 클라이언트가 AWS의 Virtual Private Cloud(VPC) 리소스에 안전하게 연결할 수 있습니다. 연결 로그를 사용하면 VPN 엔드포인트에서 사용자 활동을 추적하고 가시성을 제공할 수 있습니다. 연결 로깅을 활성화하면 로그 그룹에서 로그 스트림의 이름을 지정할 수 있습니다. 로그 스트림을 지정하지 않으면 Client VPN 서비스에서 자동으로 로그 스트림을 생성합니다.

문제 해결

연결 로깅을 활성화하려면 AWS Client VPN 관리자 안내서의 기존 Client VPN 엔드포인트에 연결 로깅 활성화를 참조하세요.

[EC2.52] EC2 전송 게이트웨이에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TransitGateway`

AWS Config 규칙: `tagged-ec2-transitgateway` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon EC2 전송 게이트웨이에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 전송 게이트웨이에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정

된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 전송 게이트웨이에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

EC2 전송 게이트웨이에 태그를 추가하려면 Amazon EC2 사용 설명서의 Amazon EC2 리소스 태깅을 참조하세요.

[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/5.3, CIS AWS 파운데이션 벤치마크 v3.0.0/5.2, PCI DSS v4.0.1/1.3.1

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: `AWS::EC2::SecurityGroup`

AWS Config 규칙: `vpc-sg-port-restriction-check`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| ipType | IP 버전 | 문자열 | 사용자 지정할 수 없음 | IPv4 |
| restrictPorts | 수신 트래픽을 거부해야 하는 포트 목록 | IntegerList | 사용자 지정할 수 없음 | 22,3389 |

이 제어는 Amazon EC2 보안 그룹이 0.0.0.0/0 또는 ::/0에서 포트(ports 22 and 3389)로의 수신을 허용하는지 확인합니다. 보안 그룹에서 0.0.0.0/0에서 포트 22 또는 3389로의 수신을 허용하면 제어가 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 어떤 보안 그룹도 TDP(6), UDP(17) 또는 ALL(-1) 프로토콜을 사용하여 SSH에서 포트 22로, RDP에서 포트 3389로 등 원격 서버 관리 포트에 대한 무제한 수신 액세스를 허용하지 않는 것이 좋습니다. 이러한 포트에 대한 퍼블릭 액세스를 허용하면 리소스 공격 표면과 리소스 손상 위험이 증가합니다.

문제 해결

지정된 포트로의 수신 트래픽을 금지하도록 EC2 보안 그룹 규칙을 업데이트하려면 Amazon EC2 사용 설명서의 보안 그룹 규칙 업데이트을 참조하세요. Amazon EC2 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 22 또는 포트 3389에 대한 액세스를 허용하는 규칙을 제거합니다.

[EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/5.4, CIS AWS 파운데이션 벤치마크 v3.0.0/5.3, PCI DSS v4.0.1/1.3.1

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: AWS::EC2::SecurityGroup

AWS Config 규칙: vpc-sg-port-restriction-check

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| ipType | IP 버전 | 문자열 | 사용자 지정 할 수 없음 | IPv6 |
| restrictPorts | 수신 트래픽을 거부해야 하는 포트 목록 | IntegerList | 사용자 지정 할 수 없음 | 22,3389 |

이 제어는 Amazon EC2 보안 그룹이 ::/0에서 원격 서버 관리 포트(포트 22 및 3389)로의 수신을 허용하는지 확인합니다. 보안 그룹에서 ::/0에서 포트 22 또는 3389로의 수신을 허용하면 제어가 실패합니다.

보안 그룹을 통해 AWS 리소스에 대한 수신 및 발신 네트워크 트래픽을 상태 저장 필터링할 수 있습니다. 어떤 보안 그룹도 TDP(6), UDP(17) 또는 ALL(-1) 프로토콜을 사용하여 SSH에서 포트 22로, RDP에서 포트 3389로 등 원격 서버 관리 포트에 대한 무제한 수신 액세스를 허용하지 않는 것이 좋습니다. 이러한 포트에 대한 퍼블릭 액세스를 허용하면 리소스 공격 표면과 리소스 손상 위험이 증가합니다.

문제 해결

지정된 포트로의 수신 트래픽을 금지하도록 EC2 보안 그룹 규칙을 업데이트하려면 Amazon EC2 사용 설명서의 보안 그룹 규칙 업데이트을 참조하세요. Amazon EC2 콘솔에서 보안 그룹을 선택한 후 작업, 인바운드 규칙 편집을 선택합니다. 포트 22 또는 포트 3389에 대한 액세스를 허용하는 규칙을 제거합니다.

[EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: AWS::EC2::VPC, AWS::EC2::VPCEndpoint

AWS Config 규칙: vpc-endpoint-enabled

스케줄 유형: 주기적

파라미터:

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|---|
| `serviceNames` | 필수 | 제어가 평가하는 서비스의 이름입니다 | 문자열 | 사용자 지정할 수 없음 | `ecr.api` |
| `vpcIds` | 선택 사항 | VPC 엔드포인트용 Amazon VPC ID의 쉼표로 구분된 목록입니다. `serviceName` 파라미터가 제공된 경우 이 파라미터에 지정된 서비스에 이러한 VPC 엔드포인트 중 하나가 없는 경우 제어가 실패합니다. | StringList | 하나 이상의 VPC ID로 사용자 지정 | 기본값 없음 |

이 제어는 관리하는 가상 프라이빗 클라우드(VPC)에 Amazon ECR API용 인터페이스 VPC 엔드포인트가 있는지 확인합니다. VPC에 ECR API용 인터페이스 VPC 엔드포인트가 없는 경우 제어가 실패합니다. 이 제어는 단일 계정의 리소스를 평가합니다.

AWS PrivateLink 를 사용하면 고객은 AWS 네트워크 내에서 모든 네트워크 트래픽을 유지하면서 가용성과 확장성이 뛰어난 방식으로 AWS 에서 호스팅되는 서비스에 액세스할 수 있습니다. 서비스 사용자는 퍼블릭 IP를 사용하지도 않고 트래픽이 인터넷을 통과할 필요도 없이 VPC 또는 온프레미스에서 PrivateLink로 구동되는 서비스에 비공개로 액세스할 수 있습니다.

문제 해결

VPC 엔드포인트를 구성하려면 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

[EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config 규칙: vpc-endpoint-enabled

스케줄 유형: 주기적

파라미터:

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|---|
| `serviceNames` | 필수 | 제어가 평가하는 서비스의 이름입니다 | 문자열 | 사용자 지정할 수 없음 | `ecr.dkr` |
| `vpcIds` | 선택 사항 | VPC 엔드포인트용 | StringList | 하나 이상의 VPC ID | 기본값 없음 |

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- | --- |
| | | Amazon VPC ID의 쉼표로 구분된 목록입니다. `serviceName` 파라미터가 제공된 경우 이 파라미터에 지정된 서비스에 이러한 VPC 엔드포인트 중 하나가 없는 경우 제어가 실패합니다. | | 로 사용자 지정 | |

이 제어는 관리하는 가상 프라이빗 클라우드(VPC)에 Docker Registry용 인터페이스 VPC 엔드포인트가 있는지 확인합니다. VPC에 Docker Registry용 인터페이스 VPC 엔드포인트가 없는 경우 제어가 실패합니다. 이 제어는 단일 계정의 리소스를 평가합니다.

AWS PrivateLink 를 사용하면 고객은 AWS 네트워크 내에서 모든 네트워크 트래픽을 유지하면서 가용성과 확장성이 뛰어난 방식으로 AWS 에서 호스팅되는 서비스에 액세스할 수 있습니다. 서비스 사용자는 퍼블릭 IP를 사용하지도 않고 트래픽이 인터넷을 통과할 필요도 없이 VPC 또는 온프레미스에서 PrivateLink로 구동되는 서비스에 비공개로 액세스할 수 있습니다.

문제 해결

VPC 엔드포인트를 구성하려면 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

[EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config 규칙: vpc-endpoint-enabled

스케줄 유형: 주기적

파라미터:

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|---|
| `serviceNames` | 필수 | 제어가 평가하는 서비스의 이름입니다 | 문자열 | 사용자 지정할 수 없음 | `ssm` |
| `vpcIds` | 선택 사항 | VPC 엔드포인트용 Amazon VPC ID의 쉼표로 구분된 목록입니다. `serviceName` 파라미터가 제공된 경우 이 | StringList | 하나 이상의 VPC ID로 사용자 지정 | 기본값 없음 |

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|---|
| | | 파라미터에 지정된 서비스에 이러한 VPC 엔드포인트 중 하나가 없는 경우 제어가 실패합니다. | | | |

이 제어는 관리하는 가상 프라이빗 클라우드(VPC)에 AWS Systems Manager용 인터페이스 VPC 엔드포인트가 있는지 확인합니다. VPC에 Systems Manager용 인터페이스 VPC 엔드포인트가 없는 경우 제어가 실패합니다. 이 제어는 단일 계정의 리소스를 평가합니다.

AWS PrivateLink 를 사용하면 고객은 AWS 네트워크 내에서 모든 네트워크 트래픽을 유지하면서 가용성과 확장성이 뛰어난 방식으로 AWS 에서 호스팅되는 서비스에 액세스할 수 있습니다. 서비스 사용자는 퍼블릭 IP를 사용하지도 않고 트래픽이 인터넷을 통과할 필요도 없이 VPC 또는 온프레미스에서 PrivateLink로 구동되는 서비스에 비공개로 액세스할 수 있습니다.

문제 해결

VPC 엔드포인트를 구성하려면 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

[EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config 규칙: vpc-endpoint-enabled

스케줄 유형: 주기적

파라미터:

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|---|
| `serviceNames` | 필수 | 제어가 평가하는 서비스의 이름입니다 | 문자열 | 사용자 지정할 수 없음 | `ssm-contacts` |
| `vpcIds` | 선택 사항 | VPC 엔드포인트용 Amazon VPC ID의 쉼표로 구분된 목록입니다. `serviceName` 파라미터가 제공된 경우 이 파라미터에 지정된 서비스에 이러한 VPC 엔드포인트 중 하나가 없는 경우 제어가 실패합니다. | StringList | 하나 이상의 VPC ID로 사용자 지정 | 기본값 없음 |

이 제어는 관리하는 Virtual Private Cloud(VPC)에 AWS Systems Manager Incident Manager Contacts에 대한 인터페이스 VPC 엔드포인트가 있는지 확인합니다. VPC에 Systems Manager Incident Manager Contacts용 인터페이스 VPC 엔드포인트가 없는 경우 제어가 실패합니다. 이 제어는 단일 계정의 리소스를 평가합니다.

AWS PrivateLink 를 사용하면 고객은 AWS 네트워크 내에서 모든 네트워크 트래픽을 유지하면서 가용성과 확장성이 뛰어난 방식으로 AWS 에서 호스팅되는 서비스에 액세스할 수 있습니다. 서비스 사용자는 퍼블릭 IP를 사용하지도 않고 트래픽이 인터넷을 통과할 필요도 없이 VPC 또는 온프레미스에서 PrivateLink로 구동되는 서비스에 비공개로 액세스할 수 있습니다.

문제 해결

VPC 엔드포인트를 구성하려면 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

[EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::EC2::VPC`, `AWS::EC2::VPCEndpoint`

AWS Config 규칙: vpc-endpoint-enabled

스케줄 유형: 주기적

파라미터:

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|---|
| `serviceNames` | 필수 | 제어가 평가하는 서 | 문자열 | 사용자 지정할 수 없음 | `ssm-incidents` |

| 파라미터 | 필수 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|---|
| | | 비스의 이름입니다 | | | |
| vpcIds | 선택 사항 | VPC 엔드포인트용 Amazon VPC ID의 쉼표로 구분된 목록입니다. serviceName 파라미터가 제공된 경우 이 파라미터에 지정된 서비스에 이러한 VPC 엔드포인트 중 하나가 없는 경우 제어가 실패합니다. | StringList | 하나 이상의 VPC ID로 사용자 지정 | 기본값 없음 |

이 제어는 관리하는 Virtual Private Cloud(VPC)에 AWS Systems Manager Incident Manager용 인터페이스 VPC 엔드포인트가 있는지 확인합니다. VPC에 Systems Manager Incident Manager용 인터페이스 VPC 엔드포인트가 없는 경우 제어가 실패합니다. 이 제어는 단일 계정의 리소스를 평가합니다.

AWS PrivateLink 를 사용하면 고객은 AWS 네트워크 내에서 모든 네트워크 트래픽을 유지하면서 가용성과 확장성이 뛰어난 방식으로 AWS 에서 호스팅되는 서비스에 액세스할 수 있습니다. 서비스 사용자는 퍼블릭 IP를 사용하지도 않고 트래픽이 인터넷을 통과할 필요도 없이 VPC 또는 온프레미스에서 PrivateLink로 구동되는 서비스에 비공개로 액세스할 수 있습니다.

문제 해결

VPC 엔드포인트를 구성하려면 AWS PrivateLink 가이드의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

[EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/2.2.6

범주: 보호 > 네트워크 보안

심각도: 낮음

리소스 유형: `AWS::EC2::LaunchTemplate`

AWS Config 규칙: ec2-launch-template-imdsv2-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 런치 템플릿이 인스턴스 메타데이터 서비스 버전 2(IMDSv2)로 구성되어 있는지 확인합니다. `HttpTokens`을 `optional`로 설정하면 제어가 실패합니다.

지원되는 소프트웨어 버전에서 리소스를 실행하면 최적의 성능, 보안 및 최신 기능에 대한 액세스를 보장할 수 있습니다. 정기 업데이트는 취약성을 방지하여 안정적이고 효율적인 사용자 경험을 보장합니다.

문제 해결

EC2 시작 템플릿에 IMDSv2가 필요하게 하려면 Amazon EC2 사용 설명서의 인스턴스 메타데이터 서비스 옵션 구성을 참조하세요.

[EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v3.0.0/5.3, PCI DSS v4.0.1/10.4.2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::EC2::VPNConnection`

AWS Config 규칙: ec2-vpn-connection-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Site-to-Site VPN 연결에 두 터널 모두에 대해 Amazon CloudWatch Logs가 활성화되어 있는지 확인합니다. Site-to-Site VPN 연결에 두 터널 모두에 대해 CloudWatch Logs가 활성화되지 않은 경우, 제어가 실패합니다.

AWS Site-to-Site VPN 로그는 Site-to-Site VPN 배포에 대한 심층적인 가시성을 제공합니다. 이 기능을 사용하면 IPsec(IP Security) 터널 설정, IKE(Internet Key Exchange) 협상 및 DPD(Dead Peer Detection) 프로토콜 메시지에 대한 세부 정보를 제공하는 Site-to-Site VPN 연결 로그에 액세스할 수 있습니다. Site-to-Site VPN 로그는 CloudWatch Logs에 게시할 수 있습니다. 이 기능은 고객이 모든 Site-to-Site VPN 연결에 대한 세부 로그를 액세스하고 분석할 수 있는 일관된 단일 방법을 제공합니다.

문제 해결

EC2 VPN 연결에서 터널 로깅을 활성화하려면 AWS Site-to-Site VPN 사용 설명서의 AWS Site-to-Site VPN 로그를 참조하세요.

[EC2.172] EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 중간

리소스 유형: `AWS::EC2::VPCBlockPublicAccessOptions`

AWS Config 규칙: `ec2-vpc-bpa-internet-gateway-blocked` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `vpcBpaInternetGatewayBlockMode` | VPC BPA 옵션 모드의 문자열 값입니다. | Enum | `block-bidirectional` , `block-ingress` | 기본값 없음 |

이 제어는 Amazon EC2 VPC 퍼블릭 액세스 차단(BPA) 설정이 AWS 계정의 모든 Amazon VPC에 대한 인터넷 게이트웨이 트래픽을 차단하도록 구성되어 있는지 확인합니다. VPC BPA 설정이 인터넷 게이트웨이 트래픽을 차단하도록 구성되지 않은 경우 제어가 실패합니다. 제어가 통과하려면 VPC BPA `InternetGatewayBlockMode`가 `block-bidirectional` 또는 `block-ingress`로 설정되어야 합니다. 파라미터 `vpcBpaInternetGatewayBlockMode`가 제공된 경우 `InternetGatewayBlockMode`의 VPC BPA 값이 파라미터와 일치하는 경우에만 제어가 통과합니다.

에서 계정에 대한 VPC BPA 설정을 구성 AWS 리전 하면 해당 리전에서 소유한 VPCs 및 서브넷의 리소스가 인터넷 게이트웨이 및 외부 전용 인터넷 게이트웨이를 통해 인터넷에 도달하거나 인터넷에서 액세스하는 것을 차단할 수 있습니다. 특정 VPC 및 서브넷이 인터넷에 연결하거나 인터넷에서 연결되어야 하는 경우 VPC BPA 제외 항목을 구성하여 제외할 수 있습니다. 제외 항목 생성 및 삭제에 대한 지침은 Amazon VPC 사용 설명서의 제외 항목 생성 및 삭제를 참조하세요.

문제 해결

계정 수준에서 양방향 BPA를 활성화하려면 Amazon VPC 사용 설명서의 계정에 대해 BPA 양방향 모드 활성화를 참조하세요. 수신 전용 BPA를 활성화하려면 VPC BPA 모드를 수신 전용으로 변경을 참조하세요. 조직 수준에서 VPC BPA를 활성화하려면 조직 수준에서 VPC BPA 활성화를 참조하세요.

[EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EC2::SpotFleet`

AWS Config 규칙: ec2-spot-fleet-request-ct-encryption-at-rest

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 시작 파라미터를 지정하는 Amazon EC2 스팟 플릿 요청이 EC2 인스턴스에 연결된 모든 Amazon Elastic Block Store(Amazon EBS) 볼륨에 대해 암호화를 활성화하도록 구성되어 있는지 확인합니다. 스팟 플릿 요청이 시작 파라미터를 지정하고 요청에 지정된 하나 이상의 EBS 볼륨에 대해 암호화를 활성화하지 않으면 제어가 실패합니다.

보안 계층을 추가하기 위해 Amazon EBS 볼륨에 대한 암호화를 활성화해야 합니다. 그러면 암호화 작업이 Amazon EC2 인스턴스를 호스팅하는 서버에서 실행되므로, 인스턴스와 연결된 Amazon EBS 스

토리지 간 전송 중 데이터와 저장 데이터 모두의 보안을 확보하는 데 도움이 됩니다. Amazon EBS 암호화는 EC2 인스턴스와 연결된 EBS 리소스를 위한 간단한 암호화 솔루션입니다. EBS 암호화를 사용하면 자체 키 관리 인프라를 구축, 유지 관리 및 보호할 필요가 없습니다. EBS 암호화는 암호화된 볼륨을 생성할 AWS KMS keys 때를 사용합니다.

> **참고**
>
> 이 제어는 시작 템플릿을 사용하는 Amazon EC2 스팟 플릿 요청에 대한 조사 결과를 생성하지 않습니다. 또한 `encrypted` 파라미터 값을 명시적으로 지정하지 않는 스팟 플릿 요청에 대해서도 조사 결과를 생성하지 않습니다.

문제 해결

기존의 암호화되지 않은 Amazon EBS 볼륨을 암호화하는 직접적인 방법은 없습니다. 새로운 볼륨을 생성할 때만 암호화할 수 있습니다.

하지만 암호화를 기본적으로 활성화한 경우 Amazon EBS는 사용자의 EBS 암호화용 기본 키를 사용하여 새로운 볼륨을 자동으로 암호화합니다. 암호화를 기본적으로 활성화하지 않더라도 개별 볼륨을 생성할 때 암호화를 활성화할 수 있습니다. 두 경우 모두 EBS 암호화용 기본 키를 재정의하고 고객 관리형 AWS KMS key를 선택할 수 있습니다. EBS 암호화에 대한 자세한 내용은 Amazon EBS 사용 설명서의 Amazon EBS 암호화를 참조하세요.

Amazon EC2 스팟 플릿 요청을 생성하는 방법에 대한 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 스팟 플릿 생성을 참조하세요.

[EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::DHCPOptions`

AWS Config 규칙: ec2-dhcp-options-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 DHCP 옵션 세트에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 옵션 세트에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 옵션 세트에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon EC2 DHCP 옵션 세트에 태그를 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태그 지정을 참조하세요.

[EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::LaunchTemplate`

AWS Config 규칙: ec2-launch-template-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 시작 템플릿에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 시작 템플릿에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 시작 템플릿에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon EC2 시작 템플릿에 태그를 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태그 지정을 참조하세요.

[EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::PrefixList`

AWS Config 규칙: ec2-prefix-list-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 접두사 목록에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 접두사 목록에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 접두사 목록에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 Tag Editor 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon EC2 접두사 목록에 태그를 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태그 지정을 참조하세요.

[EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TrafficMirrorSession`

AWS Config 규칙: ec2-traffic-mirror-session-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 트래픽 미러 세션에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 트래픽 미러 세션에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 트래픽 미러 세션에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon EC2 트래픽 미러 세션에 태그를 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태그 지정을 참조하세요.

[EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TrafficMirrorFilter`

AWS Config 규칙: ec2-traffic-mirror-filter-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 트래픽 미러 필터에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 필터에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 트래픽 미러 필터에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon EC2 트래픽 미러 필터에 태그를 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태그 지정을 참조하세요.

[EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::EC2::TrafficMirrorTarget`

AWS Config 규칙: ec2-traffic-mirror-target-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 트래픽 미러 대상에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 대상에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 대상에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon EC2 트래픽 미러 대상에 태그를 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 리소스에 태그 지정을 참조하세요.

[EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::EC2::NetworkInterface`

AWS Config 규칙: ec2-enis-source-destination-check-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 사용자가 관리하는 Amazon EC2 탄력적 네트워크 인터페이스(ENI)에 대해 소스/대상 확인이 활성화되어 있는지 확인합니다. 사용자 관리형 ENI에 대해 소스/대상 확인이 활성화되지 않은 경우 제어가 실패합니다. 이 제어는 `aws_codestar_connections_managed`, `branch`, `efa`, `interface`, `lambda` 및 `quicksight` 유형의 ENI만 확인합니다.

Amazon EC2 인스턴스 및 연결된 ENI에 대한 소스/대상 확인을 EC2 인스턴스에서 활성화하고 일관되게 구성해야 합니다. 각 ENI에는 소스/대상 확인에 대한 자체 설정이 있습니다. 소스/대상 확인이 활성화된 경우 Amazon EC2는 소스/대상 주소 검증을 적용하여 인스턴스가 수신하는 트래픽의 소스 또는 대상인지 확인합니다. 이렇게 하면 리소스가 의도하지 않은 트래픽을 처리하고 IP 주소 스푸핑을 방지하여 네트워크 보안 계층이 추가됩니다.

> **Note**
>
> EC2 인스턴스를 NAT 인스턴스로 사용하고 ENI에 대한 소스/대상 확인을 비활성화한 경우, 대신 NAT 게이트웨이를 사용할 수 있습니다.

문제 해결

Amazon EC2 ENI에 대해 소스/대상 확인을 활성화하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 네트워크 인터페이스 속성 수정을 참조하세요.

[EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EC2::LaunchTemplate`

AWS Config 규칙: ec2-launch-templates-ebs-volume-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 시작 템플릿이 모든 연결된 EBS 볼륨에 대해 암호화를 활성화하는지 확인합니다. EC2 시작 템플릿에 지정된 EBS 볼륨에 대해 암호화 파라미터가 `False`로 설정된 경우 제어가 실패합니다.

Amazon EBS 암호화는 Amazon EC2 인스턴스와 연결된 EBS 리소스를 위한 간단한 암호화 솔루션입니다. EBS 암호화를 사용하면 자체 키 관리 인프라를 구축, 유지 관리 및 보호할 필요가 없습니다. EBS 암호화는 암호화된 볼륨 및 스냅샷을 생성할 때 AWS KMS keys 를 사용합니다. 그러면 암호화 작업이 EC2 인스턴스를 호스팅하는 서버에서 실행되므로, EC2 인스턴스와 연결된 EBS 스토리지 간 전송 중 데이터와 저장 데이터 모두의 보안을 확보하는 데 도움이 됩니다. 자세한 내용은 Amazon EBS 사용 설명서의 Amazon EBS encryption을 참조하세요.

개별 EC2 인스턴스를 수동으로 시작하는 동안 EBS 암호화를 활성화할 수 있습니다. 하지만 EC2 시작 템플릿을 사용하고 해당 템플릿에서 암호화 설정을 구성하면 몇 가지 이점이 있습니다. 암호화를 표준으로 적용하고 일관된 암호화 설정을 사용할 수 있습니다. 또한 인스턴스를 수동으로 시작할 때 발생할 수 있는 오류 및 보안 격차의 위험을 줄일 수 있습니다.

> **Note**
>
> 이 제어는 EC2 시작 템플릿을 확인할 때 템플릿에 명시적으로 지정된 EBS 암호화 설정만 평가합니다. 평가에는 계정 수준 EBS 암호화 설정, AMI 블록 디바이스 매핑 또는 소스 스냅샷 암호화 상태에서 상속되는 암호화 설정은 포함되지 않습니다.

문제 해결

Amazon EC2 시작 템플릿을 생성한 후에는 수정할 수 없습니다. 그러나 새 버전의 시작 템플릿을 생성하고 이 새 버전의 템플릿에서 암호화 설정을 변경할 수 있습니다. 새 버전을 시작 템플릿의 기본 버전으로 지정할 수도 있습니다. 그런 다음 시작 템플릿에서 EC2 인스턴스를 시작할 때 템플릿 버전을 지정하지 않으면 EC2는 기본 버전의 설정을 사용하여 인스턴스를 시작합니다. 자세한 내용은 Amazon EC2 사용 설명서의 시작 템플릿 수정을 참조하세요.

[EC2.182] Amazon EBS 스냅샷에 대해 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::EC2::SnapshotBlockPublicAccess`

AWS Config 규칙: ebs-snapshot-block-public-access

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EBS 스냅샷을 모든 사람과 공유하지 못하도록 계정 수준 퍼블릭 액세스 차단이 활성화되어 있는지 확인합니다. 퍼블릭 액세스 차단이 모든에 대한 Amazon EBS 스냅샷 공유를 차단하도록 활성화되지 않은 경우 제어가 실패합니다.

Amazon EBS 스냅샷의 퍼블릭 공유를 방지하기 위해 스냅샷에 대한 퍼블릭 액세스 차단을 활성화할 수 있습니다. 리전에서 스냅샷에 대한 퍼블릭 액세스 차단이 활성화되면 해당 리전에서 스냅샷을 공개적으로 공유하려는 모든 시도가 자동으로 차단됩니다. 이렇게 하면 스냅샷의 보안을 개선하고 무단 또는 의도하지 않은 액세스로부터 스냅샷 데이터를 보호할 수 있습니다.

문제 해결

스냅샷에 대한 퍼블릭 액세스 차단을 활성화하려면 Amazon EBS 사용 설명서의 Amazon EBS 스냅샷에 대한 퍼블릭 액세스 차단 구성을 참조하세요. 퍼블릭 액세스 차단에서 모든 퍼블릭 액세스 차단을 선택합니다.

[EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EC2::VPNConnection`

AWS Config 규칙: ec2-vpn-connection-ike-version-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 IKEv2 AWS IKEv2 프로토콜을 사용하도록 Site-to-Site VPN 연결이 구성되어 있는지 확인합니다. Site-to-Site VPN 연결이 IKEv1 프로토콜을 허용하거나 모든 VPN 터널에서 IKEv2로 명시적으로 제한하지 않는 경우 제어가 실패합니다.

IKEv2는 denial-of-service 공격에 대한 기본 제공 보호 및 향상된 인증 메커니즘을 포함하여 레거시 IKEv1 프로토콜에 비해 더 강력한 암호화 알고리즘과 향상된 보안 기능을 제공합니다. IKEv1에는 공격자가 VPN 터널 보안을 손상시키기 위해 악용할 수 있는 키 교환 프로세스의 알려진 취약성과 약점이

있습니다. IKEv2-only 연결을 적용하면 공격 표면을 줄이고 VPN 통신이 최신 업계 표준 암호화 프로토콜을 사용하여 전송 중 데이터를 더 잘 보호할 수 있습니다.

문제 해결

EC2 VPN 연결에서 VPN 터널의 IKE 버전을 업데이트하려면 Site-to-Site VPN 사용 설명서의 Site-to-Site VPN 터널 옵션 수정 AWS을 참조하세요. AWS Site-to-Site

## Auto Scaling에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon EC2 Auto Scaling 서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[PCI.AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.

관련 요구 사항: 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

범주: 식별 > 인벤토리

심각도: 낮음

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: `autoscaling-group-elb-healthcheck-required`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Load Balancer와 연결된 Amazon EC2 Auto Scaling 그룹이 Elastic Load Balancing(ELB) 상태 확인을 사용하고 있는지 확인합니다. Auto Scaling 그룹이 ELB 상태 확인을 사용하지 않으면 제어가 실패합니다.

ELB 상태 확인은 Auto Scaling 그룹에서 로드 밸런서가 제공하는 추가 테스트에 따라 인스턴스 상태를 확인할 수 있습니다. Elastic Load Balancing 상태 확인을 사용하면 EC2 Auto Scaling 그룹을 사용하는 애플리케이션의 가용성을 지원하는 데 도움이 될 수 있습니다.

문제 해결

Elastic Load Balancing 상태 확인을 추가하려면 Amazon EC2 Auto Scaling 사용 설명서 의 Elastic Load Balancing 상태 확인 추가를 참조하세요.

[AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: `autoscaling-multiple-az`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `minAvailabilityZones` | 최소 가용 영역의 수 | Enum | `2, 3, 4, 5, 6` | `2` | |

이 제어는 Amazon EC2 Auto Scaling 그룹이 지정된 수 이상의 가용 영역(AZ)에 걸쳐 있는지 확인합니다. Auto Scaling 그룹이 최소한 지정된 수의 AZ에 걸쳐 있지 않으면 제어가 실패합니다. 최소 AZs 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 2개의 AZs 사용합니다.

여러 AZ에 걸쳐 있지 않은 Auto Scaling 그룹은 구성된 단일 AZ를 사용할 수 없게 될 경우, 이를 보완하기 위해 다른 AZ에서 인스턴스를 시작할 수 없습니다. 하지만 일괄 작업이나 AZ 간 전송 비용을 최소로 유지해야 하는 경우와 같은 일부 사용 사례에서는 단일 가용 영역이 있는 Auto Scaling 그룹이 선호될 수 있습니다. 이 경우, 이 제어를 비활성화하거나 조사 결과를 숨길 수 있습니다.

문제 해결

기존 Auto Scaling 그룹에 AZ를 추가하려면 Amazon EC2 Auto Scaling 사용 설명서의 가용 영역 추가 및 제거를 참조하세요.

[AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::AutoScaling::LaunchConfiguration`

AWS Config 규칙: `autoscaling-launchconfig-requires-imdsv2`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 Auto Scaling 그룹에서 시작한 모든 인스턴스에서 IMDSv2가 활성화되어 있는지 확인합니다. 인스턴스 메타데이터 서비스(IMDS) 버전이 시작 구성에 포함되지 않거나 IMDSv1 또는 IMDSv2를 허용하는 설정인 `token optional`로 구성된 경우, 제어가 실패합니다.

IMDS는 실행 중인 인스턴스를 구성하거나 관리하는 데 사용할 수 있는 인스턴스에 대한 데이터를 제공합니다.

IMDS 버전 2에는 IMDSv1에서 사용할 수 없었던 새로운 보호 기능이 추가되어 EC2 인스턴스를 더욱 안전하게 보호할 수 있습니다.

문제 해결

Auto Scaling 그룹 은 한 번에 한 개의 시작 구성과 연결됩니다. 시작 구성을 생성한 후에는 수정할 수 없습니다. Auto Scaling 그룹의 시작 구성을 변경하려면 기존 시작 구성을 IMDSv2가 활성화된 새로운 시작 구성의 기초로 사용합니다. 자세한 내용은 Amazon EC2 사용 설명서의 새로운 인스턴스에 대한 인스턴스 메타데이터 옵션 구성을 참조하세요.

[AutoScaling.4] Auto Scaling 그룹 시작 구성에는 1보다 큰 메타데이터 응답 홉 제한이 있어서는 안 됩니다

> **Important**
>
> Security Hub CSPM은 2024년 4월에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그 단원을 참조하십시오.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::AutoScaling::LaunchConfiguration`

AWS Config 규칙: `autoscaling-launch-config-hop-limit`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 메타데이터 토큰이 이동할 수 있는 네트워크 홉 수를 확인합니다. 메타데이터 응답 홉 제한이 1보다 크면 제어가 실패합니다.

인스턴스 메타데이터 서비스(IMDS)는 Amazon EC2 인스턴스에 대한 메타데이터 정보를 제공하며 애플리케이션 구성에 유용합니다. 메타데이터 서비스에 대한 HTTP PUT 응답을 EC2 인스턴스로만 제한하면 IMDS를 무단으로 사용하지 못하도록 보호할 수 있습니다.

IP 패킷의 TTL(Time To Live) 필드는 모든 홉에서 1씩 감소됩니다. 이렇게 감소되면 패킷이 EC2 외부로 이동하지 않도록 할 수 있습니다. IMDSv2는 개방형 라우터, 계층 3 방화벽, VPN, 터널 또는 NAT 디바이스로 잘못 구성되었을 수 있는 EC2 인스턴스를 보호하여 권한이 없는 사용자가 메타데이터를 검색하지 못하도록 합니다. IMDSv2를 사용하면 기본 메타데이터 응답 홉 제한이 1로 설정되어 있기 때문에 비밀 토큰이 포함된 PUT 응답이 인스턴스 외부로 이동할 수 없습니다. 하지만 이 값이 1보다 크면 토큰이 EC2 인스턴스를 벗어날 수 있습니다.

문제 해결

기존 시작 구성의 메타데이터 응답 홉 제한을 수정하려면 Amazon EC2 사용 설명서의 기존 인스턴스에 대한 인스턴스 메타데이터 옵션 수정을 참조하세요.

[Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::AutoScaling::LaunchConfiguration`

AWS Config 규칙: `autoscaling-launch-config-public-ip-disabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Auto Scaling 그룹 의 관련 시작 구성이 그룹 인스턴스에 퍼블릭 IP 주소를 할당하는지 여부를 확인합니다. 연결된 시작 구성이 퍼블릭 IP 주소를 할당하면 제어가 실패합니다.

Auto Scaling 그룹 시작 구성의 Amazon EC2 인스턴스에는 제한된 엣지 케이스를 제외하고 연결된 퍼블릭 IP 주소가 없어야 합니다. Amazon EC2 인스턴스는 인터넷에 직접 노출되지 않고 로드 밸런서 뒤에서만 액세스할 수 있어야 합니다.

문제 해결

Auto Scaling 그룹 은 한 번에 한 개의 시작 구성과 연결됩니다. 시작 구성을 생성한 후에는 수정할 수 없습니다. 기존 Auto Scaling 그룹의 시작 구성을 변경하기 위해 기존 시작 구성을 새로운 시작 구성의 기초로 사용할 수 있습니다. 그런 다음 새로운 시작 구성을 사용하도록 Auto Scaling 을 업데이트합니다. 단계별 지침은 Amazon EC2 Auto Scaling 사용 설명서에서 Auto Scaling 그룹 에 대한 시작 구성 변경을 참조하세요. 새로운 시작 구성을 생성할 때, 추가 구성에서 고급 세부 정보, IP 주소 유형에서 어떤 인스턴스에도 퍼블릭 IP 주소를 할당하지 않음을 선택합니다.

시작 구성을 변경한 후 Auto Scaling은 새 구성 옵션을 사용하여 새로운 인스턴스를 시작합니다. 기존 인스턴스는 영향을 받지 않습니다. 기존 인스턴스를 업데이트하려면 인스턴스를 새로 고치거나 자동 조정을 허용하여 종료 정책에 따라 이전 인스턴스를 새로운 인스턴스로 점진적으로 교체하는 것이 좋습니다. Auto Scaling 인스턴스 업데이트에 대한 자세한 내용은 Amazon EC2 Auto Scaling 사용 설명서의 Auto Scaling 인스턴스 업데이트를 참조하세요.

[AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config 규칙: autoscaling-multiple-instance-types

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 Auto Scaling 그룹이 여러 인스턴스 유형을 사용하는지 여부를 확인합니다. Auto Scaling 그룹 에 정의된 인스턴스 유형이 하나만 있는 경우, 제어가 실패합니다.

여러 가용 영역에서 실행되는 여러 인스턴스 유형에 애플리케이션을 배포하여 가용성을 높일 수 있습니다. Security Hub CSPM은 선택한 가용 영역에 인스턴스 용량이 부족한 경우 Auto Scaling 그룹이 다른 인스턴스 유형을 시작할 수 있도록 여러 인스턴스 유형을 사용할 것을 권장합니다.

문제 해결

여러 인스턴스 유형이 포함된 Auto Scaling 그룹 을 생성하려면 Amazon EC2 Auto Scaling 사용 설명서의 여러 인스턴스 유형 및 구매 옵션이 포함된 오토 스케일링을 참조하세요.

[오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: AWS::AutoScaling::AutoScalingGroup

AWS Config 규칙: autoscaling-launch-template

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EC2 Auto Scaling 그룹 이 EC2 시작 템플릿에서 생성되었는지 여부를 확인합니다. Amazon EC2 Auto Scaling 그룹 이 시작 템플릿으로 생성되지 않았거나 혼합 인스턴스 정책에 시작 템플릿이 지정되지 않은 경우, 이 제어가 실패합니다.

EC2 Auto Scaling 그룹 은 EC2 시작 템플릿이나 시작 구성에서 생성할 수 있습니다. 하지만 시작 템플릿을 사용하여 Auto Scaling 그룹 을 생성하면 최신 기능과 개선 사항을 이용할 수 있습니다.

문제 해결

EC2 시작 템플릿을 사용하여 Auto Scaling 그룹 을 생성하려면 Amazon EC2 Auto Scaling 사용 설명서의 시작 템플릿을 사용하여 오토 스케일링 생성을 참조하세요. 시작 구성을 시작 템플릿으로 바꾸는

방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 시작 구성을 시작 템플릿으로 교체를 참조하세요.

[AutoScaling.10] EC2 Auto Scaling 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::AutoScaling::AutoScalingGroup`

AWS Config규칙: `tagged-autoscaling-autoscalinggroup` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EC2 Auto Scaling 그룹에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. Auto Scaling 그룹에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 Auto Scaling 그룹에 키로 태그가 지정되지 않으면 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Auto Scaling 그룹에 태그를 추가하려면 Amazon EC2 Auto Scaling 사용 설명서의 태그 Auto Scaling 그룹 및 인스턴스를 참조하세요.

## Amazon ECR에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon Elastic Container Registry(Amazon ECR) 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 RA-5, PCI DSS v4.0.1/6.2.3, PCI DSS v4.0.1/6.2.4

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::ECR::Repository`

AWS Config 규칙: ecr-private-image-scanning-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 프라이빗 Amazon ECR 리포지토리에 이미지 스캔이 구성되어 있는지 확인합니다. 프라이빗 ECR 리포지토리가 푸시 시 스캔 또는 연속 스캔에 대해 구성되지 않은 경우, 제어가 실패합니다.

ECR 이미지 스캔은 컨테이너 이미지의 소프트웨어 취약성을 식별하는 데 도움이 됩니다. ECR 리포지토리에서 이미지 스캔을 구성하면 저장되는 이미지의 무결성과 안전성에 대한 검증 계층이 추가됩니다.

문제 해결

ECR 리포지토리의 이미지 스캔을 구성하려면 Amazon Elastic Container 레지스트리 사용 설명서의 이미지 스캔을 참조하세요.

[ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-8(1)

범주: 식별 > 인벤토리 > 태그 지정

심각도: 중간

리소스 유형: `AWS::ECR::Repository`

AWS Config 규칙: ecr-private-tag-immutability-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 프라이빗 ECR 리포지토리에 태그 불변성이 활성화되어 있는지 확인합니다. 프라이빗 ECR 리포지토리에 태그 불변성이 비활성화된 경우, 이 제어가 실패합니다. 이 규칙은 태그 불변성이 활성화되고 값이 `IMMUTABLE`인 경우, 통과됩니다.

Amazon ECR Tag Immuability를 사용하면 고객은 이미지를 추적하고 고유하게 식별하는 안정적인 메커니즘으로 이미지 설명 태그를 활용할 수 있습니다. 불변 태그는 정적입니다. 즉, 각 태그는 고유한 이미지를 참조합니다. 정적 태그를 사용하면 항상 동일한 이미지가 배포되므로 안정성과 확장성이 향상됩니다. 태그 불변성을 구성하면 태그 불변성으로 인해 태그가 재정의되지 않아 공격 표면이 줄어듭니다.

문제 해결

변경할 수 없는 태그가 구성된 리포지토리를 만들거나 기존 리포지토리의 이미지 태그 변경 가능성 설정을 업데이트하려면 Amazon Elastic Container Registry 사용 설명서의 이미지 태그 변경 가능성을 참조하세요.

[ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::ECR::Repository`

AWS Config 규칙: ecr-private-lifecycle-policy-configured

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECR 리포지토리에 하나 이상의 수명 주기 정책이 구성되어 있는지 확인합니다. ECR 저장소에 수명 주기 정책이 구성되어 있지 않으면 이 제어가 실패합니다.

Amazon ECR 수명 주기 정책을 통해 리포지토리의 이미지에 대한 수명 주기 관리를 지정할 수 있습니다. 수명 주기 정책을 구성하면 사용하지 않는 이미지의 정리 및 사용 기간 또는 개수에 따른 이미지 만료를 자동화할 수 있습니다. 이러한 작업을 자동화하면 저장소에서 오래된 이미지를 실수로 사용하는 것을 방지할 수 있습니다.

문제 해결

수명 주기 정책을 구성하려면 Amazon Elastic Container Registry 사용 설명서의 수명 주기 정책 미리 보기 생성을 참조하세요.

[ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::ECR::PublicRepository`

AWS Config 규칙: `tagged-ecr-publicrepository` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon ECR 퍼블릭 리포지토리에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 퍼블릭 리포지토리에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 퍼블릭 리포지토리에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

ECR 퍼블릭 리포지토리에 태그를 추가하려면 Amazon Elastic Container Registry 사용 설명서의 Amazon ECR 퍼블릭 리포지토리 태그 지정을 참조하세요.

[ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ECR::Repository`

AWS Config 규칙: ecr-repository-cmk-encryption-enabled

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `kmsKeyArns` | 평가에 AWS KMS keys 포함할의 Amazon 리소스 이름(ARNs) 목록입니다. ECR 리포지토리가 목록의 KMS 키로 암호화되지 않은 경우, 제어는 `FAILED` 조사 결과를 생성합니다. | StringList(최대 10개 항목) | 기존 KMS 키의 ARN 1~10개. 예: `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` | 기본값 없음 |

이 제어는 Amazon ECR 리포지토리가 고객 관리형 AWS KMS key로 저장 시 암호화되는지 확인합니다. ECR 리포지토리가 고객 관리형 KMS 키로 암호화되지 않은 경우 제어가 실패합니다. 선택적으로 평가에 포함할 제어에 대한 KMS 키 목록을 지정할 수 있습니다.

기본적으로 Amazon ECR은 AES-256 알고리즘을 사용하여 Amazon S3 관리형 키(SSE-S3)로 리포지토리 데이터를 암호화합니다. 추가 제어를 위해 대신 AWS KMS key (SSE-KMS 또는 DSSE-KMS)를 사용하여 데이터를 암호화하도록 Amazon ECR을 구성할 수 있습니다. KMS 키는 Amazon ECR이 생성 및 관리하고 별칭 `aws/ecr`이 있는 AWS 관리형 키 또는 AWS 계정에서 생성 및 관리하는 고객 관리형 키일 수 있습니다. 고객 관리형 KMS 키를 사용하면 고객이 키를 완전히 제어할 수 있습니다. 여기에는 키 정책 정의 및 유지 관리, 권한 부여 관리, 암호화 자료 교체, 태그 할당, 별칭 생성, 키 활성화 및 비활성화가 포함됩니다.

> **Note**
>
> AWS KMS 는 KMS 키에 대한 교차 계정 액세스를 지원합니다. ECR 리포지토리가 다른 계정이 소유한 KMS 키로 암호화된 경우 이 제어는 리포지토리를 평가할 때 교차 계정 확인을 수행하지 않습니다. 제어는 Amazon ECR이 리포지토리에 대한 암호화 작업을 수행할 때 키에 액세스하고 사용할 수 있는지 여부를 평가하지 않습니다.

문제 해결

기존 ECR 리포지토리의 암호화 설정은 변경할 수 없습니다. 그러나 이후에 생성하는 ECR 리포지토리에 대해 다른 암호화 설정을 지정할 수 있습니다. Amazon ECR은 개별 리포지토리에 다양한 암호화 설정을 사용하도록 지원합니다.

ECR 리포지토리의 암호화 옵션에 대한 자세한 내용은 Amazon ECR 사용 설명서의 저장 시 암호화를 참조하세요. 고객 관리형에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서AWS KMS keys의 섹션을 AWS KMS keys참조하세요.

## Amazon ECS에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon Elastic Container Service(Amazon ECS) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::ECS::Service`

AWS Config규칙: `ecs-service-assign-public-ip-disabled` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 서비스가 퍼블릭 IP 주소를 자동으로 할당하도록 구성되었는지 여부를 확인합니다. 이 제어는 `AssignPublicIP`가 `ENABLED`인 경우, 실패합니다. 이 제어는 `AssignPublicIP`가 `DISABLED`인 경우, 통과됩니다.

퍼블릭 IP 주소는 인터넷을 통해 연결할 수 있는 IPv 주소입니다. 퍼블릭 IP 주소로 Amazon ECS 인스턴스를 시작하면 인터넷에서 Amazon ECS 인스턴스에 연결할 수 있습니다. Amazon ECS 서비스는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 컨테이너 애플리케이션 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

문제 해결

먼저 `awsvpc` 네트워크 모드를 사용하고 `requiresCompatibilities`에 대해 FARGATE을 지정하는 클러스터에 대한 작업 정의를 생성해야 합니다. 그런 다음 컴퓨팅 구성에서 시작 유형 및 FARGATE를 선택합니다. 마지막으로 네트워킹 필드에서 퍼블릭 IP를 꺼서 서비스에 대한 자동 퍼블릭 IP 할당을 비활성화합니다.

[ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 식별 > 리소스 구성

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-task-definition-pid-mode-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 작업 정의가 호스트의 프로세스 네임스페이스를 컨테이너와 공유하도록 구성되어 있는지 확인합니다. 태스크 정의가 호스트의 프로세스 네임스페이스를 호스트에서 실행되는 컨테이너와 공유하면 제어가 실패합니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

프로세스 ID(PID) 네임스페이스는 프로세스 간 분리를 제공합니다. 시스템 프로세스가표시되는 것을 방지하고 PID 1을 포함한 PID를 재사용할 수 있습니다. 호스트의 PID 네임스페이스를 컨테이너와 공유하면 컨테이너는 호스트 시스템의 모든 프로세스를 볼 수 있습니다. 이렇게 하면 호스트와 컨테이너 간의 프로세스 수준 격리의 이점이 줄어듭니다. 이러한 상황에서는 프로세스를 조작하고 종료하는 기

능을 포함하여 호스트 자체에 있는 프로세스에 대한 무단 액세스가 발생할 수 있습니다. 고객은 호스트의 프로세스 네임스페이스를 호스트에서 실행되는 컨테이너와 공유해서는 안 됩니다.

문제 해결

태스크 정의에 대해 `pidMode`를 구성하려면 Amazon Elastic Container Service 개발자 안내서의 태스크 정의 파라미터를 참조하세요.

[ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 루트 사용자 액세스 제한

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-containers-nonprivileged

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 태스크 정의의 컨테이너 정의에 있는 `privileged` 파라미터가 `true`로 설정되어 있는지 확인합니다. 이 파라미터가 `true`과 같으면 제어가 실패합니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

ECS 태스크 정의에서 상승된 권한을 제거하는 것이 좋습니다. 권한 파라미터가 `true`인 경우, 컨테이너는 호스트 컨테이너 인스턴스에 대해 상승된 권한을 부여받습니다(루트 사용자와 비슷함).

문제 해결

태스크 정의에 대한 `privileged` 파라미터를 구성하려면 Amazon Elastic Container Service 개발자 안내서의 고급 컨테이너 정의 파라미터를 참조하세요.

[ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-containers-readonly-access

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 ECS 태스크 정의가 탑재된 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성하는지 여부를 확인합니다. ECS 작업 정의의 컨테이너 정의에 있는 `readonlyRootFilesystem` 파라미터가 로 설정`false`되거나 파라미터가 작업 정의 내의 컨테이너 정의에 없는 경우 제어가 실패합니다. 이 제어는 Amazon ECS 태스크 정의의 최신 활성 개정만 평가합니다.

Amazon ECS 태스크 정의에서 `readonlyRootFilesystem` 파라미터가 `true`로 설정된 경우 ECS 컨테이너에는 루트 파일 시스템에 대한 읽기 전용 액세스 권한이 부여됩니다. 이렇게 하면 파일 시스템 폴더 및 디렉터리에 대한 읽기-쓰기 권한이 있는 명시적 볼륨 탑재 없이는 컨테이너 인스턴스의 루트 파일 시스템에 쓰거나 변조할 수 없으므로 보안 공격 벡터가 줄어듭니다. 이 옵션을 활성화하면 최소 권한 원칙도 준수합니다.

> **Note**
>
> `readonlyRootFilesystem` 파라미터는 Windows 컨테이너에서 지원되지 않습니다. `WINDOWS_SERVER` OS 패밀리를 지정하도록 `runtimePlatform` 구성된 작업 정의는 로 표시`NOT_APPLICABLE`되며이 컨트롤에 대한 결과를 생성하지 않습니다.

문제 해결

Amazon ECS 컨테이너에 루트 파일 시스템에 대한 읽기 전용 액세스 권한을 부여하려면 컨테이너의 태스크 정의에 `readonlyRootFilesystem` 파라미터를 추가하고 파라미터 값을 `true`로 설정합니다. 태스크 정의 파라미터와 이를 태스크 정의에 추가하는 방법에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 태스크 정의 및 태스크 정의 업데이트를 참조하세요.

[ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/8.6.2

범주: 보호 > 보안 개발 > 하드 코딩되지 않은 보안 인증

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-no-environment-secrets

스케줄 유형: 변경이 트리거됨

파라미터: `secretKeys`: `AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY,ECS_ENGINE_AUTH_DATA`(사용자 지정할 수 없음)

이 제어는 컨테이너 정의의 `environment` 파라미터에 있는 변수의 키 값에 `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` 또는 `ECS_ENGINE_AUTH_DATA`가 포함되어 있는지 확인합니다. 컨테이너 정의의 단일 환경 변수가 `AWS_ACCESS_KEY_ID`, `AWS_SECRET_ACCESS_KEY` 또는 `ECS_ENGINE_AUTH_DATA`와 같으면 이 제어가 실패합니다. 이 제어에는 Amazon S3와 같은 다른 위치에서 전달된 환경 변수는 포함되지 않습니다. 이 제어는 Amazon ECS 작업 정의의 최신 활성 개정만 평가합니다.

AWS Systems ManagerParameter Store는 조직의 보안 태세를 개선하는 데 도움이 될 수 있습니다. 암호와 보안 인증을 컨테이너 인스턴스로 직접 전달하거나 코드에 하드 코딩하는 대신 Parameter Store를 사용하여 암호와 보안 인증을 저장하는 것이 좋습니다.

문제 해결

SSM을 사용하여 파라미터를 생성하려면 AWS Systems Manager 사용 설명서의 Systems Manager 파라미터 생성을 참조하세요. 암호를 지정하는 작업 정의 생성에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 Secrets Manager를 사용하여 중요한 데이터 지정을 참조하세요.

[ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-task-definition-log-configuration

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어 최신 활성 Amazon ECS 작업 정의에 로깅 구성이 지정되어 있는지 확인합니다. 작업 정의에 정의된 `logConfiguration` 속성이 없거나 하나 이상의 컨테이너 정의에서 `logDriver`의 값이 null인 경우, 제어가 실패합니다.

로깅은 Amazon ECS의 안정성, 가용성 및 성능을 유지하는 데 도움이 됩니다. 작업 정의에서 데이터를 수집하면 가시성이 제공되므로 프로세스를 디버깅하고 오류의 근본 원인을 찾는 데 도움이 됩니다. ECS 작업 정의에 정의할 필요가 없는 로깅 솔루션(예: 타사 로깅 솔루션)을 사용하는 경우, 로그가 제대로 캡처되고 전달되었는지 확인한 후 이 제어를 비활성화할 수 있습니다.

문제 해결

Amazon ECS 작업 정의의 로그 구성을 정의하려면 Amazon Elastic Container Service 개발자 안내서의 작업 정의에 로그 구성 지정을 참조하세요.

[ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.

관련 요구 사항: 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::ECS::Service`

AWS Config 규칙: ecs-fargate-latest-platform-version

스케줄 유형: 변경이 트리거됨

파라미터:

- `latestLinuxVersion: 1.4.0`(사용자 지정할 수 없음)
- `latestWindowsVersion: 1.0.0`(사용자 지정할 수 없음)

이 제어는 Amazon ECS Fargate 서비스가 최신 Fargate 플랫폼 버전을 실행하고 있는지 확인합니다. 플랫폼 버전이 최신 버전이 아닌 경우, 이 제어가 실패합니다.

AWS Fargate플랫폼 버전은 커널 및 컨테이너 런타임 버전의 조합인 Fargate 작업 인프라의 특정 런타임 환경을 나타냅니다. 런타임 환경이 발전함에 따라 새로운 플랫폼 버전이 출시됩니다. 예를 들어, 커

널 또는 운영 체제 업데이트, 새로운 기능, 버그 수정 또는 보안 업데이트용으로 새 버전이 릴리스될 수 있습니다. 보안 업데이트 및 패치는 Fargate 태스크에서 자동 배포됩니다. 플랫폼 버전에 영향을 미치는 보안 문제가 발견되면는 플랫폼 버전을 AWS패치합니다.

문제 해결

플랫폼 버전을 비롯한 기존 서비스를 업데이트하려면 Amazon Elastic Container Service 개발자 안내서의 서비스 업데이트를 참조하세요.

[ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ECS::Cluster`

AWS Config 규칙: ecs-container-insights-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 ECS 클러스터가 컨테이너 인사이트를 사용하는지 확인합니다. Container Insights가 클러스터에 설정되지 않은 경우, 이 제어는 실패합니다.

모니터링은 Amazon ECS 클러스터의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. CloudWatch Container Insights를 사용해 컨테이너화된 애플리케이션 및 마이크로서비스의 메트릭 및 로그를 수집하고 집계하며 요약할 수 있습니다. CloudWatch는 CPU, 메모리, 디스크, 네트워크와 같은 많은 리소스에 대한 메트릭를 자동으로 수집합니다. 또한 Container Insights는 컨테이너 재시작 오류 같은 진단 정보를 제공하여 문제를 격리하고 신속하게 해결할 수 있도록 도와줍니다. Container Insights가 수집하는 메트릭에 대해 CloudWatch 경보를 설정할 수도 있습니다.

문제 해결

Container Insights를 사용하려면 Amazon CloudWatch 사용 설명서의 서비스 업데이트를 참조하세요.

[ECS.13] ECS 서비스에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::ECS::Service`

AWS Config규칙: `tagged-ecs-service` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어 검사는 Amazon ECS 서비스에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 서비스에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 서비스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

ECS 서비스에 태그를 추가하려면 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 리소스 태그 지정을 참조하세요.

[ECS.14] ECS 클러스터에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::ECS::Cluster`

AWS Config규칙: `tagged-ecs-cluster` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon ECS 클러스터에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 클러스터에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 클러스터에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수

있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

ECS 클러스터에 태그를 추가하려면 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 리소스 태그 지정을 참조하세요.

[ECS.15] ECS 작업 정의에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config규칙: `tagged-ecs-taskdefinition` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon ECS 태스크 정의에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 태스크 정의에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든

키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 작업 정의에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

ECS 작업 정의에 태그를 추가하려면 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 리소스 태그 지정을 참조하세요.

[ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.

관련 요구 사항: PCI DSS v4.0.1/1.4.4

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::ECS::TaskSet`

AWS Config규칙: `ecs-taskset-assign-public-ip-disabled` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 작업 세트가 퍼블릭 IP 주소를 자동으로 할당하도록 구성되었는지 여부를 확인합니다. `AssignPublicIP`을 `ENABLED`로 설정하면 제어가 실패합니다.

퍼블릭 IP 주소는 인터넷을 통해 연결할 수 있는 주소입니다. 퍼블릭 IP 주소로 작업 세트를 구성하는 경우, 인터넷에서 작업 세트와 연결된 리소스에 연결할 수 있습니다. ECS 작업 세트는 공개적으로 액세스할 수 없어야 합니다. 이렇게 하면 컨테이너 애플리케이션 서버에 의도하지 않은 액세스가 허용될 수 있기 때문입니다.

문제 해결

퍼블릭 IP 주소를 사용하지 않도록 ECS 태스크 세트를 업데이트하려면 Amazon Elastic Container Service 개발자 안내서의 콘솔을 사용하여 Amazon ECS 태스크 정의 업데이트 섹션을 참조하세요.

[ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-task-definition-network-mode-not-host

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 태스크 정의의 최신 활성 개정이 `host` 네트워크 모드를 사용하는지 확인합니다. ECS 태스크 정의의 최신 활성 개정에서 `host` 네트워크 모드를 사용하는 경우 제어가 실패합니다.

`host` 네트워크 모드를 사용하면 Amazon ECS 컨테이너의 네트워킹이 컨테이너를 실행 중인 기본 호스트에 직접 연결됩니다. 따라서, 이 모드를 사용하면 컨테이너가 호스트의 프라이빗 루프백 네트워크 서비스에 연결하고 호스트를 가장할 수 있습니다. 다른 중요한 단점은 `host` 네트워크 모드를 사용할 때 컨테이너 포트를 다시 매핑할 방법이 없으며 각 호스트에서 태스크를 한 번 이상 인스턴스화할 수 없다는 것입니다.

문제 해결

Amazon EC2 인스턴스에서 호스팅되는 Amazon ECS 태스크의 네트워킹 모드 및 옵션에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 EC2 시작 유형을 위한 Amazon ECS 태스

크 네트워킹 옵션을 참조하세요. 태스크 정의의 새 개정을 생성하고 다른 네트워크 모드를 지정하는 방법에 대한 자세한 내용은 해당 안내서의 Amazon ECS 태스크 정의 업데이트를 참조하세요.

에서 Amazon ECS 작업 정의를 생성한 경우 네트워킹 모드 및 AWS Batch작업 유형의 일반적인 사용에 대해 알아보고 보안 옵션을 선택하려면 AWS Batch작업의 네트워킹 모드를 AWS Batch참조하세요.

[ECS.18] ECS 작업 정의는 EFS 볼륨에 대해 전송 중 암호화를 사용해야 합니다.

범주: 보호 > 데이터 보호 > 전송 중 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-task-definition-efs-encryption-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 태스크 정의의 최신 활성 개정이 EFS 볼륨에 전송 중 암호화를 사용하는지 확인합니다. ECS 태스크 정의의 최신 활성 개정에 EFS 볼륨에 대해 전송 중 암호화가 비활성화된 경우 제어가 실패합니다.

Amazon EFS 볼륨은 Amazon ECS 작업에 사용할 수 있는 간단하고 확장 가능하며 영구적인 공유 파일 스토리지를 제공합니다. Amazon EFS는 Transport Layer Security(TLS)를 통한 전송 중 데이터 암호화를 지원합니다. 전송 중 데이터 암호화가 EFS 파일 시스템의 탑재 옵션으로 선언되면 Amazon EFS는 파일 시스템을 탑재할 때 EFS 파일 시스템과 안전한 TLS 연결을 설정합니다.

문제 해결

EFS 볼륨을 사용하여 Amazon ECS 작업 정의에 대한 전송 중 암호화를 활성화하는 방법에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 5단계: 작업 정의 생성을 참조하세요.

[ECS.19] ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호

심각도: 중간

리소스 유형: `AWS::ECS::CapacityProvider`

AWS Config 규칙: ecs-capacity-provider-termination-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 용량 공급자가 관리형 종료 방지 기능을 활성화했는지 확인합니다. ECS 용량 공급자에서 관리형 종료 보호가 활성화되지 않은 경우 제어가 실패합니다.

Amazon ECS 용량 공급자는 클러스터의 작업에 대한 인프라의 조정을 관리할 수 있습니다. 용량으로 EC2 인스턴스를 사용하는 경우 Auto Scaling 그룹을 사용하여 EC2 인스턴스를 관리합니다. 관리형 종료 보호 기능을 사용하면 클러스터 Auto Scaling을 통해 종료되는 인스턴스를 제어할 수 있습니다. 관리형 종료 보호 기능을 사용한 경우 Amazon ECS는 실행 중인 Amazon ECS 태스크가 없는 EC2 인스턴스만 종료합니다.

> **Note**
>
> 관리형 종료 방지 기능을 사용하는 경우 관리형 확장도 사용해야 합니다. 그렇지 않으면 관리형 종료 방지 기능이 작동하지 않습니다.

문제 해결

Amazon ECS 용량 공급자에 대한 관리형 종료 보호를 활성화하려면 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 용량 공급자에 대한 관리형 종료 보호 업데이트를 참조하세요.

[ECS.20] ECS 작업 정의는 Linux 컨테이너 정의에서 루트가 아닌 사용자를 구성해야 합니다.

범주: 보호 > 보안 액세스 관리 > 루트 사용자 액세스 제한

심각도: 중간

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-task-definition-linux-user-non-root

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 태스크 정의의 최신 활성 개정이 루트가 아닌 사용자로 실행되도록 Linux 컨테이너를 구성하는지 확인합니다. 컨테이너에 대해 기본 루트 사용자가 구성되거나 사용자 구성이 없는 경우 제어가 실패합니다.

Linux 컨테이너가 루트 권한으로 실행되면 몇 가지 중요한 보안 위험이 발생합니다. 루트 사용자는 컨테이너 내에서 무제한 액세스 권한을 갖습니다. 이렇게 액세스 권한이 높아지면 공격자가 컨테이너 격리를 해제하고 기본 호스트 시스템에 액세스할 수 있는 컨테이너 이스케이프 공격의 위험이 높아집니다. 루트로 실행되는 컨테이너가 손상된 경우 공격자는 이를 사용하여 호스트 시스템 리소스에 액세스하거나 수정하여 다른 컨테이너 또는 호스트 자체에 영향을 미칠 수 있습니다. 또한 루트 액세스는 권한 에스컬레이션 공격을 활성화하여 공격자가 컨테이너의 의도한 범위를 벗어나는 추가 권한을 얻을 수 있습니다. ECS 태스크 정의의 사용자 파라미터는 사용자 이름, 사용자 ID, 그룹이 있는 사용자 이름 또는 그룹 ID가 있는 UID 등 여러 형식으로 사용자를 지정할 수 있습니다. 실수로 루트 액세스 권한이 부여되지 않도록 태스크 정의를 구성할 때 이러한 다양한 형식을 알고 있어야 합니다. 최소 권한 원칙에 따라 컨테이너는 루트가 아닌 사용자를 사용하여 필요한 최소 권한으로 실행되어야 합니다. 이 접근 방식은 잠재적 공격 표면을 크게 줄이고 잠재적 보안 침해의 영향을 완화합니다.

> **Note**
>
> 이 제어는 `operatingSystemFamily`가 작업 정의에 `LINUX` 또는 로 구성되어 `operatingSystemFamily` 있지 않은 경우에만 작업 정의의 컨테이너 정의를 평가합니다. 태스크 정의의 컨테이너 정의가 기본 루트 사용자`user`로 구성`user`되지 않은 경우, 제어는 평가된 태스크 정의에 대한 `FAILED` 결과를 생성합니다. `LINUX` 컨테이너의 기본 루트 사용자는 `"root"` 및 입니다`"0"`.

문제 해결

Amazon ECS 작업 정의의 새 개정을 생성하고 컨테이너 정의에서 `user` 파라미터를 업데이트하는 방법에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 작업 정의 업데이트를 참조하세요.

[ECS.21] ECS 작업 정의는 Windows 컨테이너 정의에서 관리자가 아닌 사용자를 구성해야 합니다.

범주: 보호 > 보안 액세스 관리 > 루트 사용자 액세스 제한

심각도: 중간

리소스 유형: `AWS::ECS::TaskDefinition`

AWS Config 규칙: ecs-task-definition-windows-user-non-admin

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon ECS 태스크 정의의 최신 활성 개정이 기본 관리자가 아닌 사용자로 실행되도록 Windows 컨테이너를 구성하는지 확인합니다. 기본 관리자가 사용자로 구성되거나 컨테이너에 사용자 구성이 없는 경우 제어가 실패합니다.

Windows 컨테이너가 관리자 권한으로 실행되면 몇 가지 중요한 보안 위험이 발생합니다. 관리자는 컨테이너 내에서 무제한 액세스 권한을 갖습니다. 이렇게 액세스 권한이 높아지면 공격자가 컨테이너 격리를 해제하고 기본 호스트 시스템에 액세스할 수 있는 컨테이너 이스케이프 공격의 위험이 높아집니다.

> **Note**
>
> 이 제어는 `operatingSystemFamily`가 작업 정의에서 `WINDOWS_SERVER` 또는 로 구성되어 `operatingSystemFamily` 있지 않은 경우에만 작업 정의의 컨테이너 정의를 평가합니다. 태스크 정의의 컨테이너 정의가 인 컨테이너의 기본 관리자로 구성되지 않았거나 `user` 구성`user`되지 않은 경우, 제어`WINDOWS_SERVER`는 평가된 태스크 정의에 대한 `FAILED` 결과를 생성합니다`"containeradministrator"`.

문제 해결

Amazon ECS 작업 정의의 새 개정을 생성하고 컨테이너 정의에서 `user` 파라미터를 업데이트하는 방법에 대한 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 Amazon ECS 작업 정의 업데이트를 참조하세요.

## Amazon EFS에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon Elastic File System(Amazon EFS) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.3.1, CIS AWS 파운데이션 벤치마크 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: AWS::EFS::FileSystem

AWS Config 규칙: efs-encrypted-check

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Elastic File System이를 사용하여 파일 데이터를 암호화하도록 구성되어 있는지 확인합니다 AWS KMS. 다음과 같은 경우에는 확인에 실패합니다.

- Encrypted는 DescribeFileSystems 응답에서 false로 설정됩니다.
- DescribeFileSystems 응답의 KmsKeyId 키가 efs-encrypted-check의 KmsKeyId 파라미터와 일치하지 않습니다.

참고로 이 제어는 efs-encrypted-check에 KmsKeyId 파라미터를 사용하지 않습니다. 이는 Encrypted 값만 확인합니다.

Amazon EFS의 중요한 데이터에 대한 보안 계층을 추가하려면 암호화된 파일 시스템을 생성해야 합니다. Amazon EFS는 저장 중인 파일 시스템에 대한 암호화를 지원합니다. Amazon EFS 파일 시스템을 생성할 때 저장 데이터 암호화를 활성화할 수 있습니다. Amazon EFS 암호화에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 Amazon EFS의 데이터 암호화를 참조하세요.

문제 해결

새로운 Amazon EFS 파일 시스템을 암호화하는 방법에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 미사용 데이터 암호화를 참조하세요.

[EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 백업

심각도: 중간

리소스 유형: AWS::EFS::FileSystem

AWS Config 규칙: efs-in-backup-plan

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Elastic File System(Amazon EFS) 파일 시스템이 AWS Backup의 백업 계획에 추가되었는지 확인합니다. Amazon EFS 파일 시스템이 백업 계획에 포함되지 않은 경우, 제어가 실패합니다.

백업 계획에 EFS 파일 시스템을 포함하면 데이터가 삭제되거나 손실되지 않도록 보호할 수 있습니다.

문제 해결

기존 Amazon EFS 파일 시스템의 자동 백업을 활성화하려면 AWS Backup 개발자 안내서의 시작하기 4: Amazon EFS 자동 백업 생성을 참조하세요.

[EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-6(10)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::EFS::AccessPoint`

AWS Config 규칙: efs-access-point-enforce-root-directory

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EFS 액세스 포인트가 루트 디렉터리를 적용하도록 구성되어 있는지 확인합니다. `Path`의 값을 `/`(파일 시스템의 기본 루트 디렉터리)로 설정하면 제어가 실패합니다.

루트 디렉터리를 적용할 때 액세스 포인트를 사용하는 NFS 클라이언트는 파일 시스템의 루트 디렉터리 대신 액세스 포인트에 구성된 루트 디렉터리를 사용합니다. 액세스 포인트에 루트 디렉터리를 적용하면 액세스 포인트의 사용자가 지정된 하위 디렉터리의 파일에만 액세스할 수 있도록 하여 데이터 액세스를 제한하는 데 도움이 됩니다.

문제 해결

Amazon EFS 액세스 포인트에 루트 디렉터리를 적용하는 방법에 대한 지침은 Amazon Elastic File System 사용 설명서의 액세스 포인트를 사용하여 루트 디렉터리 적용을 참조하세요.

[EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-6(2), PCI DSS v4.0.1/7.3.1

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::EFS::AccessPoint`

AWS Config 규칙: efs-access-point-enforce-user-identity

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EFS 액세스 포인트가 사용자 ID를 적용하도록 구성되었는지 여부를 확인합니다. EFS 액세스 포인트를 생성하는 동안 POSIX 사용자 ID가 정의되지 않으면 이 제어가 실패합니다.

Amazon EFS 액세스 포인트는 EFS 파일 시스템에 대한 애플리케이션별 진입점으로, 공유 데이터 세트에 대한 애플리케이션 액세스를 더 쉽게 관리할 수 있도록 합니다. 액세스 포인트는 액세스 포인트를 통해 이루어지는 모든 파일 시스템 요청에 대해 사용자의 POSIX 그룹을 포함한 사용자 ID를 적용할 수 있습니다. 또한 클라이언트가 지정된 디렉터리 또는 하위 디렉터리의 데이터에만 액세스할 수 있도록 파일 시스템에 대해 다른 루트 디렉터리를 적용할 수 있습니다.

문제 해결

Amazon EFS 액세스 포인트에 대한 사용자 ID를 적용하려면 Amazon Elastic File System 사용 설명서의 액세스 포인트를 사용하여 사용자 ID 적용을 참조하세요.

[EFS .5] EFS 액세스 포인트에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::EFS::AccessPoint`

AWS Config규칙: `tagged-efs-accesspoint` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EFS 액세스 포인트에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 액세스 포인트에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 액세스 포인트에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

EFS 액세스 포인트에 태그를 추가하려면 Amazon Elastic File System 사용 설명서의 Amazon EFS 리소스 태그 지정을 참조하세요.

[EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다

관련 요구 사항: NIST.800-53.r5 SC-7, NIST.800-171.r2 3.1.20, PCI DSS v4.0.1/1.4.4

범주: 보호 > 네트워크 보안 > 공개적으로 액세스할 수 없는 리소스

심각도: 중간

리소스 유형: `AWS::EFS::FileSystem`

AWS Config 규칙: efs-mount-target-public-accessible

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EFS 탑재 대상이 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어 있는지 확인합니다. 탑재 대상이 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결된 경우 제어가 실패합니다.

서브넷에는 서브넷에서 생성된 네트워크 인터페이스가 퍼블릭 IP 주소를 자동으로 수신할지 여부를 결정하는 속성이 있습니다. IPv4의 경우 기본 서브넷의 `TRUE` 경우 `MapPublicIpOnLaunch` 속성이 로 설정되고 기본이 아닌 서브넷의 `FALSE` 경우 속성이 로 설정됩니다(EC2 인스턴스 시작 마법사를 통해 생성된 기본이 아닌 서브넷의 경우 예외, 여기서 로 설정됨`TRUE`). IPv6의 경우 `AssignIpv6AddressOnCreation` 속성은 기본적으로 모든 서브넷에 `FALSE` 대해 로 설정됩니다.

Amazon EFS 탑재 대상에 퍼블릭 IPv4 주소를 할당할 수 없지만 시작 시 퍼블릭 IP 주소를 할당하도록 구성된 서브넷에 대상을 배치하면 EFS 파일 시스템을 탑재할 수 있는 해당 서브넷에서 시작된 공동 위치 인스턴스가 퍼블릭 IP 주소를 자동으로 수신할 수 있으며, 이로 인해 퍼블릭 주소 호스트에서 파일 시스템 데이터에 액세스할 수 있게 될 위험이 있습니다.

퍼블릭 IPv6 주소 자동 할당이 활성화된 서브넷에 대상을 탑재하면 전역적으로 라우팅 가능한 IPv6 주소를 수신할 수 있습니다.

> **Note**
>
> 2026년 8월 3일에 Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에서이 제어를 제거했습니다. 이 제어는 NIST SP 800-53 개정 5 표준, NIST SP 800-171 개정 2 표준 및 PCI DSS v4.0.1 표준에서 사용할 수 있습니다.

문제 해결

기존 탑재 대상을 다른 서브넷과 연결하려면 시작 시 퍼블릭 IP 주소를 할당하지 않는 서브넷에서 새 탑재 대상을 생성한 다음 이전 탑재 대상을 제거해야 합니다. 보안 그룹 및 탑재 대상에 관한 자세한 내용은 Amazon Elastic 파일 시스템 사용 설명서의 탑재 대상 및 보안 그룹 생성과 관리를 참조하세요.

[EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::EFS::FileSystem`

AWS Config 규칙: efs-automatic-backups-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EFS 파일 시스템에 자동 백업이 활성화되어 있는지 확인합니다. EFS 파일 시스템에 자동 백업이 활성화되지 않은 경우, 이 제어는 실패합니다.

데이터 백업은 원본과 별도로 저장된 시스템, 구성 또는 애플리케이션 데이터의 사본입니다. 정기 백업을 활성화하면 시스템 장애, 사이버 공격 또는 우발적 삭제와 같은 예상치 못한 이벤트로부터 중요한 데이터를 보호할 수 있습니다. 또한 강력한 백업 전략을 갖추면 데이터 손실이 발생할 수 있으므로 복구, 비즈니스 연속성 및 안심할 수 있습니다.

문제 해결

EFS 파일 시스템에 AWS Backup 를 사용하는 방법에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 EFS 파일 시스템 백업을 참조하세요. Amazon Elastic File System

[EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.3.1

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EFS::FileSystem`

AWS Config 규칙: efs-filesystem-ct-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EFS 파일 시스템이 AWS Key Management Service ()를 사용하여 데이터를 암호화하는지 확인합니다AWS KMS. 파일 시스템을 암호화하지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 저장 데이터를 암호화하면 기밀성을 보호할 수 있으므로 권한이 없는 사용자가 데이터에 액세스할 수 있는 위험이 줄어듭니다.

문제 해결

새로운 Amazon EFS 파일 시스템을 저장 시 암호화하는 방법에 대한 자세한 내용은 Amazon Elastic File System 사용 설명서의 저장 시 데이터 암호화를 참조하세요.

## Amazon EKS에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon Elastic Kubernetes Service(Amazon EKS) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: eks-endpoint-no-public-access

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EKS 클러스터 엔드포인트에 공개적으로 액세스할 수 있는지 여부를 확인합니다. EKS 클러스터에 공개적으로 액세스할 수 있는 엔드포인트가 있는 경우, 제어가 실패합니다.

새로운 클러스터를 생성하면 Amazon EKS는 클러스터와 통신하는 데 사용하는 관리형 Kubernetes API 서버에 대한 엔드포인트를 생성합니다. 기본적으로 이 API 서버 엔드포인트는 인터넷에 공개적으로 사용할 수 있습니다. API 서버에 대한 액세스는 AWS Identity and Access Management (IAM)과 네

이티브 Kubernetes 역할 기반 액세스 제어(RBAC)의 조합을 사용하여 보호됩니다. 엔드포인트에 대한 퍼블릭 액세스를 제거하면 클러스터에 대한 의도하지 않은 노출 및 액세스를 방지할 수 있습니다.

문제 해결

기존 EKS 클러스터의 엔드포인트 액세스를 수정하려면 Amazon EKS 사용 설명서의 클러스터 엔드포인트 액세스 수정을 참조하세요. 새로운 EKS 클러스터를 생성할 때 해당 클러스터에 대한 엔드포인트 액세스를 설정할 수 있습니다. 새로운 Amazon EKS 클러스터 생성에 대한 지침은 Amazon EKS 사용 설명서의 Amazon EKS 클러스터 생성을 참조하세요.

[EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.

관련 요구 사항: 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: eks-cluster-supported-version

스케줄 유형: 변경이 트리거됨

파라미터:

- `oldestVersionSupported`: `1.34`(사용자 지정할 수 없음)

이 제어는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터가 표준 지원 Kubernetes 버전에서 실행 중인지 확인합니다. Amazon EKS 클러스터가 지원되지 않거나 확장된 지원 버전에서 실행 중인 경우 제어가 실패합니다.

애플리케이션에 특정 버전의 Kubernetes가 필요하지 않은 경우, 클러스터에 대해 EKS에서 지원하는 사용 가능한 최신 Kubernetes 버전을 사용하는 것이 좋습니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS Kubernetes 릴리스 일정 및 Amazon EKS의 Kubernetes 버전 수명 주기 이해를 참조하세요.

문제 해결

EKS 클러스터를 업데이트하려면 Amazon EKS 사용 설명서의 기존 클러스터를 새 Kubernetes 버전으로 업데이트를 참조하세요.

[EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: eks-cluster-secrets-encrypted

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EKS 클러스터가 암호화된 Kubernetes 보안 암호를 사용하는지 확인합니다. 클러스터의 Kubernetes 보안 암호가 암호화되지 않으면 제어가 실패합니다.

보안 암호를 암호화할 때 AWS Key Management Service (AWS KMS) 키를 사용하여 클러스터의 etcd에 저장된 Kubernetes 보안 암호의 봉투 암호화를 제공할 수 있습니다. 이 암호화는 EKS 클러스터의 일부로 etcd에 저장된 모든 데이터(보안 암호 포함)에 대해 기본적으로 활성화되는 EBS 볼륨 암호화에 추가됩니다. EKS 클러스터에 보안 암호 암호화를 사용하면 정의 및 관리하는 KMS 키로 Kubernetes 보안 암호를 암호화하여 Kubernetes 애플리케이션에 대한 심층 방어 전략을 배포할 수 있습니다.

> **Note**
>
> 이 제어는 2026년 8월 10일 이후에 사용 중지되며 해당하는 모든 Security Hub CSPM 표준에서 제거됩니다. Kubernetes 버전 1.28부터 Amazon EKS 클러스터에는 기본적으로 봉투 암호화로 보호되는 Kubernetes 보안 암호가 있습니다.

문제 해결

EKS 클러스터에서 보안 암호 암호화를 활성화하려면 Amazon EKS 사용 설명서의 기존 클러스터에서 보안 암호 암호화 활성화를 참조하세요.

[EKS.6] EKS 클러스터에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: `tagged-eks-cluster` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EKS 클러스터에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 클러스터에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 클러스터에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

EKS 클러스터에 태그를 추가하려면 Amazon EKS 사용 설명서의 Amazon EKS 리소스 태그 지정을 참조하세요.

[EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::EKS::IdentityProviderConfig`

AWS Config 규칙: `tagged-eks-identityproviderconfig` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EKS ID 제공업체 구성에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 구성에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 구성에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에

태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

EKS ID 제공업체 구성에 태그를 추가하려면 Amazon EKS 사용 설명서의 Amazon EKS 리소스 태그 지정을 참조하세요.

[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::EKS::Cluster`

AWS Config 규칙: eks-cluster-log-enabled

스케줄 유형: 변경이 트리거됨

파라미터:

- `logTypes: audit`(사용자 지정할 수 없음)

이 제어는 Amazon EKS 클러스터에 감사 로깅이 활성화되어 있는지 여부를 확인합니다. 클러스터에 감사 로깅이 활성화되어 있지 않으면 제어가 실패합니다.

> **Note**
>
> 이 제어는 AWS 계정에 대해 Amazon Security Lake를 통해 Amazon EKS 감사 로깅이 활성화되었는지 여부를 확인하지 않습니다.

EKS 컨트롤 플레인 로깅은 EKS 컨트롤 플레인에서 계정의 Amazon CloudWatch Logs로 감사 및 진단 로그를 직접 제공합니다. 필요한 로그 유형을 선택할 수 있으며, 로그는 CloudWatch의 각 EKS 클러스터에 대한 그룹에 로그 스트림으로 전송됩니다. 로깅은 EKS 클러스터의 액세스 및 성능에 대한 가시성을 제공합니다. EKS 클러스터의 EKS 컨트롤 플레인 로그를 CloudWatch Logs로 전송하면 중앙 위치에서 감사 및 진단 목적으로 작업을 기록할 수 있습니다.

문제 해결

EKS 클러스터의 감사 로그를 활성화하려면 Amazon EKS 사용 설명서의 컨트롤 플레인 로그 활성화 및 비활성화를 참조하세요.

[EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::EKS::Nodegroup`

AWS Config 규칙: eks-nodegroup-supported-version-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `oldestVersionSupported`: `1.34`(사용자 지정할 수 없음)

이 제어는 Amazon EKS 노드 그룹이 표준 지원 Kubernetes 버전에서 실행되는지 확인합니다. Amazon EKS 노드 그룹이 지원되지 않거나 확장된 지원 버전에서 실행되는 경우 제어가 실패합니다.

지원되지 않는 Kubernetes 버전에서 EKS 노드 그룹을 실행하면 해당 노드가 더 이상 보안 패치, 버그 수정 또는 호환성 업데이트를 받지 않습니다 AWS. 지원되지 않는 버전에는 최신 릴리스에서 해결된 알려진 취약성이 포함될 수 있으며, Kubernetes 에코시스템의 업데이트된 AWS 서비스컨테이너 이미지 및 타사 도구와의 호환성 문제가 발생할 수 있습니다. 애플리케이션에 특정 버전의 Kubernetes가 필요하지 않은 경우 노드 그룹에 대해 Amazon EKS에서 지원하는 사용 가능한 최신 Kubernetes 버전을

사용하는 것이 좋습니다. 자세한 내용은 Amazon EKS 사용 설명서의 Amazon EKS Kubernetes 릴리스 일정 및 노드 업데이트의 각 단계 이해를 참조하세요.

문제 해결

EKS 노드 그룹을 업데이트하려면 Amazon EKS 사용 설명서의 클러스터의 관리형 노드 그룹 업데이트를 참조하세요.

## ElastiCache에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon ElastiCache 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 백업 활성화

심각도: 높음

리소스 유형: `AWS::ElastiCache::CacheCluster`, `AWS:ElastiCache:ReplicationGroup`

AWS Config 규칙: elasticache-redis-cluster-automatic-backup-check

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `snapshotRetentionPeriod` | 최소 스냅샷 보존 기간(일수) | Integer | `1~35` | 1 |

이 제어는 Amazon ElastiCache(Redis OSS) 클러스터에 자동 백업이 활성화되어 있는지 평가합니다. Redis OSS 클러스터의 `SnapshotRetentionLimit`가 지정된 기간 미만이면 제어가 실패합니다. 스

냅샷 보존 기간 동안 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 1일을 사용합니다.

ElastiCache(Redis OSS) 클러스터는 데이터를 백업할 수 있습니다. 클러스터를 복원하거나 새로운 클러스터를 시드하기 위해 백업을 사용할 수 있습니다. 백업은 클러스터에 저장된 모든 데이터와 클러스터의 메타데이터로 구성됩니다. 모든 백업은 Amazon S3에 쓰여지므로 내구성 있는 스토리지가 확보됩니다. 새로운 ElastiCache 클러스터를 생성하고 백업 데이터로 채워 데이터를 복원할 수 있습니다. AWS Management Console, AWS CLI및 ElastiCache API를 사용하여 백업을 관리할 수 있습니다.

> **Note**
>
> 또한 이 제어는 ElastiCache(Redis OSS 및 Valkey) 복제 그룹을 평가합니다.

문제 해결

ElastiCache 클러스터에서 자동 백업을 예약하는 방법에 대한 자세한 내용은 Amazon ElastiCache 사용 설명서의 자동 백업 예약을 참조하세요.

[ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다

관련 요구 사항: 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::ElastiCache::CacheCluster`

AWS Config 규칙: elasticache-auto-minor-version-upgrade-check

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon ElastiCache가 마이너 버전 업그레이드를 캐시 클러스터에 자동으로 적용하는지 여부를 평가합니다. 캐시 클러스터에 마이너 버전 업그레이드가 자동으로 적용되지 않으면 이 제어가 실패합니다.

> **Note**
>
> 이 제어는 ElastiCache Memcached 클러스터에는 적용되지 않습니다.

마이너 버전 자동 업그레이드는 새로운 마이너 캐시 엔진 버전을 사용할 수 있을 때 캐시 클러스터가 자동으로 업그레이드되도록 Amazon ElastiCache에서 활성화할 수 있는 기능입니다. 이러한 업그레이드에는 보안 패치 및 버그 수정이 포함될 수 있습니다. 패치 설치를 통해 최신 상태를 유지하는 것은 시스템 보안을 유지하기 위한 중요한 단계입니다.

문제 해결

기존 ElastiCache 캐시 클러스터에 자동으로 마이너 버전 업그레이드를 적용하려면 Amazon ElastiCache 사용 설명서의 ElastiCache 버전 관리를 참조하세요.

[ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: elasticache-repl-grp-auto-failover-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 ElastiCache 복제 그룹에 자동 장애 조치가 활성화되어 있는지 확인합니다. 복제 그룹에 자동 장애 조치가 활성화되어 있지 않으면 이 제어가 실패합니다.

복제 그룹에 대해 자동 장애 조치가 활성화된 경우, 기본 노드의 역할은 자동으로 읽기 전용 복제본 중 하나로 장애 조치됩니다. 이러한 장애 조치 및 복제본 승격을 통해 승격이 완료된 후 새로운 기본 복제본에 대한 쓰기를 재개할 수 있으므로 실패 시 전체 가동 중지 시간이 줄어듭니다.

문제 해결

기존 ElastiCache 복제 그룹에 대해 자동 장애 조치를 활성화하려면 Amazon ElastiCache 사용 설명서의 ElastiCache 클러스터 수정을 참조하세요. ElastiCache 콘솔을 사용하는 경우, 자동 장애 조치를 활성화됨으로 설정하세요.

[ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: elasticache-repl-grp-encrypted-at-rest

스케줄 유형: 주기적

파라미터: 없음

이 제어는 ElastiCache 복제 그룹이 저장 시 암호화되는지 확인합니다. 복제 그룹이 저장 시 암호화되지 않으면 제어가 실패합니다.

데이터를 저장 시 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. ElastiCache(Redis OSS)복제 그룹은 추가 보안 계층을 위해 저장 시 암호화되어야 합니다.

문제 해결

ElastiCache 복제 그룹에서 저장 시 암호화를 구성하려면 Amazon ElastiCache 사용 설명서의 저장 시 암호화 활성화를 참조하세요.

[ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: elasticache-repl-grp-encrypted-in-transit

스케줄 유형: 주기적

파라미터: 없음

이 제어는 ElastiCache 복제 그룹이 전송 중 암호화되는지 확인합니다. 복제 그룹이 전송 중 암호화되지 않으면 제어가 실패합니다.

전송 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다. ElastiCache 복제 그룹에서 전송 중 암호화를 활성화하면 클러스터의 노드 간 또는 클러스터와 애플리케이션 간 등 데이터가 한 위치에서 다른 위치로 이동할 때마다 데이터가 암호화됩니다.

문제 해결

ElastiCache 복제 그룹에서 전송 중 암호화를 구성하려면 Amazon ElastiCache 사용 설명서의 전송 중 암호화 활성화를 참조하세요.

[ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::ElastiCache::ReplicationGroup`

AWS Config 규칙: elasticache-repl-grp-redis-auth-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 ElastiCache(Redis OSS) 복제 그룹에 Redis OSS AUTH가 활성화되어 있는지 확인합니다. 해당 복제 그룹 노드의 Redis OSS 버전이 6.0 미만이고 `AuthToken`이 사용되지 않는 경우, 제어가 실패합니다.

Redis 인증 토큰 또는 비밀번호를 사용하는 경우, Redis는 클라이언트가 명령을 실행하도록 허용하기 전에 비밀번호를 요구하므로 데이터 보안이 향상됩니다. Redis 6.0 이상 버전의 경우, RBAC(역할 기반 액세스 제어)를 사용하는 것이 좋습니다. 6.0 이전의 Redis 버전에서는 RBAC가 지원되지 않으므로 이 제어는 RBAC 기능을 사용할 수 없는 버전만 평가합니다.

문제 해결

ElastiCache(Redis OSS) 복제 그룹에서 Redis AUTH를 사용하려면 Amazon ElastiCache 사용 설명서의 기존 ElastiCache(Redis OSS) 클러스터에서 AUTH 토큰 수정을 참조하세요.

[ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::ElastiCache::CacheCluster`

AWS Config 규칙: elasticache-subnet-group-check

스케줄 유형: 주기적

파라미터: 없음

이 제어는 ElastiCache 클러스터가 사용자 지정 서브넷 그룹으로 구성되어 있는지 확인합니다. ElastiCache 클러스터에 대한 `CacheSubnetGroupName`에 `default` 값이 있는 경우, 제어가 실패합니다.

ElastiCache 클러스터를 시작할 때 기본 서브넷 그룹이 아직 없는 경우, 기본 서브넷 그룹이 생성됩니다. 기본 그룹은 기본 Virtual Private Cloud(VPC)의 서브넷을 사용합니다. 클러스터가 있는 서브넷과 클러스터가 서브넷에서 상속하는 네트워킹을 더욱 제한하는 사용자 지정 서브넷 그룹을 사용하는 것이 좋습니다.

문제 해결

ElastiCache 클러스터를 위한 새로운 서브넷 그룹을 생성하려면 Amazon ElastiCache 사용 설명서의 서브넷 그룹 생성을 참조하세요.

## Elastic Beanstalk에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWS Elastic Beanstalk서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7,NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::ElasticBeanstalk::Environment`

AWS Config 규칙: `beanstalk-enhanced-health-reporting-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Elastic Beanstalk 환경에 향상된 상태 보고가 활성화되어 있는지 여부를 확인합니다.

Elastic Beanstalk의 향상된 상태 보고 기능을 사용하면 기본 인프라의 상태 변화에 보다 신속하게 대응할 수 있습니다. 이러한 변경으로 인해 애플리케이션 가용성이 떨어질 수 있습니다.

Elastic Beanstalk 고급 상태 보고는 식별된 문제의 심각도를 측정하고 조사할 수 있는 가능한 원인을 식별할 수 있는 상태 설명자를 제공합니다. 지원되는 Amazon 머신 이미지(AMI)에 포함된 Elastic Beanstalk 상태 에이전트는 환경 EC2 인스턴스의 로그와 메트릭를 평가합니다.

자세한 내용은 AWS Elastic Beanstalk 개발자 안내서의 향상된 상태 보고 및 모니터링을 참조하세요.

문제 해결

향상된 상태 보고를 활성화하는 방법에 대한 지침은 AWS Elastic Beanstalk 개발자 안내서의 Elastic Beanstalk 콘솔을 사용하여 향상된 상태 보고 활성화를 참조하세요.

[ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.

관련 요구 사항: 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::ElasticBeanstalk::Environment`

AWS Config 규칙: `elastic-beanstalk-managed-updates-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `UpdateLevel` | 버전 업데이트 수준 | Enum | `minor`, `patch` | 기본값 없음 |

이 제어는 Elastic Beanstalk 환경에 대해 관리형 플랫폼 업데이트가 활성화되었는지 여부를 확인합니다. 관리형 플랫폼 업데이트가 활성화되지 않은 경우, 제어가 실패합니다. 기본적으로 모든 유형의 플랫폼 업데이트가 활성화되면 제어가 통과됩니다. 필요에 따라 특정 업데이트 수준을 요구하는 사용자 지정 파라미터 값을 제공할 수 있습니다.

관리형 플랫폼 업데이트를 활성화하면 해당 환경에 사용 가능한 최신 플랫폼 수정 사항, 업데이트 및 기능이 설치됩니다. 패치 설치를 최신 상태로 유지하는 것은 시스템 보안의 중요한 단계입니다.

문제 해결

관리형 플랫폼 업데이트를 활성화하려면 AWS Elastic Beanstalk 개발자 안내서의 관리형 플랫폼 업데이트에서 관리형 플랫폼 업데이트를 구성하려면을 참조하세요.

[ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/10.4.2

범주: 식별 > 로깅

심각도: 높음

리소스 유형: `AWS::ElasticBeanstalk::Environment`

AWS Config 규칙: elastic-beanstalk-logs-to-cloudwatch

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| RetentionInDays | 만료 전 로그 이벤트를 유지할 일수 | Enum | 1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365 , 400, 545, 731, 1827, 3653 | 기본값 없음 |

이 제어는 Elastic Beanstalk 환경이 로그를 CloudWatch Logs로 전송하도록 구성되어 있는지 여부를 확인합니다. Elastic Beanstalk 환경이 로그를 CloudWatch Logs로 전송하도록 구성되지 않은 경우, 제어가 실패합니다. 필요에 따라 만료 전 지정된 일 수 동안 로그가 보존되는 경우에만 제어가 통과되도록 하려면 RetentionInDays 파라미터에 대한 사용자 지정 값을 제공하면 됩니다.

CloudWatch를 사용하면 애플리케이션 및 인프라 리소스에 대한 다양한 메트릭를 수집하고 모니터링할 수 있습니다. CloudWatch를 사용하여 특정 메트릭를 기반으로 경보 작업을 구성할 수도 있습니다. Elastic Beanstalk 환경에 대한 가시성을 높이려면 Elastic Beanstalk를 CloudWatch와 통합하는 것이 좋습니다. Elastic Beanstalk 로그에는 eb-activity.log, nginx 또는 Apache 프록시 서버 환경의 액세스 로그, 환경별 로그가 포함됩니다.

문제 해결

Elastic Beanstalk를 CloudWatch Logs와 통합하려면 AWS Elastic Beanstalk 개발자 가이드의 CloudWatch Logs로 인스턴스 로그 스트리밍을 참조하세요.

## Elastic Load Balancing에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Elastic Load Balancing 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.

관련 요구 사항: 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)

범주: 감지 > 감지 서비스

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: alb-http-to-https-redirection-check

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Application Load Balancer의 모든 HTTP 리스너에 HTTP에서 HTTPS로의 리디렉션이 구성되어 있는지 확인합니다. Application Load Balancer의 HTTP 리스너 중 하나라도 HTTP에서 HTTPS로의 리디렉션이 구성되어 있지 않으면 제어가 실패합니다.

Application Load Balancer를 사용하기 전에 리스너를 하나 이상 추가해야 합니다. 리스너는 구성한 프로토콜 및 포트를 사용하여 연결 요청을 확인하는 프로세스입니다. 리스너는 HTTP 및 HTTPS 프로토콜 모두를 지원합니다. HTTPS 리스너를 사용하여 암호화 및 암호 해독 작업을 로드 밸런서로 오프로드할 수 있습니다. 전송 중 암호화를 적용하려면 Application Load Balancer와 함께 리디렉션 작업을 사용하여 클라이언트 HTTP 요청을 포트 443의 HTTPS 요청으로 리디렉션해야 합니다.

자세한 정보는 Application Load Balancers 사용 설명서의 Application Load Balancer용 리스너를 참조하세요.

문제 해결

HTTP 요청을 HTTPS로 리디렉션하려면 Application Load Balancer 리스너 규칙을 추가하거나 기존 규칙을 편집해야 합니다.

새로운 규칙을 추가하는 방법에 대한 지침은 Application Load Balancer 사용 설명서의 규칙 추가를 참조하세요. 프로토콜: 포트의 경우, HTTP를 선택한 다음 **80**를 입력합니다. 작업 추가, 리디렉션 대상에서 HTTPS를 선택한 다음 **443**를 입력합니다.

기존 규칙을 편집하는 방법에 대한 지침은 Application Load Balancer 사용 설명서의 규칙 편집을 참조하세요. 프로토콜: 포트의 경우, HTTP를 선택한 다음 **80**를 입력합니다. 작업 추가, 리디렉션 대상에서 HTTPS를 선택한 다음 **443**를 입력합니다.

[ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: elb-acm-certificate-required

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Certificate Manager (ACM)에서 제공하는 HTTPS/SSL 인증서를 Classic Load Balancer에서 사용하는지 여부를 확인합니다. HTTPS/SSL 리스너로 구성된 Classic Load Balancer가 ACM에서 제공한 인증서를 사용하지 않는 경우, 제어가 실패합니다.

인증서를 생성하려면 ACM이나 SSL 및 TLS 프로토콜을 지원하는 도구(예: OpenSSL)를 사용할 수 있습니다. Security Hub CSPM은 ACM을 사용하여 로드 밸런서에 대한 인증서를 생성하거나 가져올 것을 권장합니다.

ACM은 Classic Load Balancer와 통합되므로 로드 밸런서에 인증서를 배포할 수 있습니다. 또한 이러한 인증서를 자동으로 갱신해야 합니다.

문제 해결

ACM SSL/TLS 인증서를 Classic Load Balancer와 연결하는 방법에 대한 자세한 내용은 AWS 지식 센터 문서 ACM SSL/TLS 인증서를 Classic, Application 또는 Network Load Balancer와 연결하려면 어떻게 해야 합니까?를 참조하세요.

[ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.

관련 요구 사항: 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 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: elb-tls-https-listeners-only

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Classic Load Balancer 리스너가 프런트엔드(클라이언트에서 로드 밸런서로) 연결을 위해 HTTPS 또는 TLS 프로토콜로 구성되어 있는지 확인합니다. 이 제어는 Classic Load Balancer에 리스너가 있는 경우, 적용할 수 있습니다. Classic Load Balancer에 리스너가 구성되어 있지 않은 경우, 제어는 조사 결과를 보고하지 않습니다.

Classic Load Balancer 리스너가 프런트 엔드 연결용 TLS 또는 HTTPS로 구성된 경우, 제어가 통과됩니다.

리스너가 프런트엔드 연결에 대해 TLS 또는 HTTPS로 구성되지 않은 경우, 제어가 실패합니다.

로드 밸런서 사용을 시작하기 전에 하나 이상의 리스너를 추가해야 합니다. 리스너는 구성한 프로토콜 및 포트를 사용하여 연결 요청을 확인하는 프로세스입니다. 리스너는 HTTP 및 HTTPS/TLS 프로토콜을 모두 지원합니다. 로드 밸런서가 전송 중에 암호화 및 복호화 작업을 수행하도록 하려면 항상 HTTPS 또는 TLS 리스너를 사용해야 합니다.

문제 해결

이 문제를 해결하려면 TLS 또는 HTTPS 프로토콜을 사용하도록 리스너를 업데이트하세요.

모든 비준수 리스너를 TLS/HTTPS 리스너로 변경하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창의 로드 밸런싱에서 로드 밸런서를 선택합니다.

3. Classic Load Balancer를 선택합니다.
4. 리스너 탭에서 편집을 선택합니다.
5. 로드 밸런서 프로토콜이 HTTPS 또는 SSL로 설정되지 않은 모든 리스너의 경우, 설정을 HTTPS 또는 SSL로 변경합니다.
6. 수정된 모든 리스너의 경우, 인증서 탭에서 기본값 변경을 선택합니다.
7. ACM 및 IAM 인증서에서 인증서를 선택합니다.
8. 기본값으로 저장을 선택합니다.
9. 리스너를 모두 업데이트한 후 저장을 선택합니다.

[ELB.4] Application Load Balancer는 잘못된 http 헤더를 삭제하도록 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 SC-7(4), NIST.800-53.r5 SC-8(2), PCI DSS v4.0.1/6.2.4

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: alb-http-drop-invalid-header-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Application Load Balancer를 평가하여 잘못된 HTTP 헤더를 삭제하도록 구성되었는지 확인합니다. `routing.http.drop_invalid_header_fields.enabled` 값이 `false`로 설정되면 제어가 실패합니다.

기본적으로 Application Load Balancer는 잘못된 HTTP 헤더 값을 삭제하도록 구성되지 않습니다. 이러한 헤더 값을 제거하면 HTTP 비동기화 공격이 방지됩니다.

> **Note**
>
> 계정에서 ELB.12가 활성화된 경우, 이 제어를 비활성화하는 것이 좋습니다. 자세한 내용은 [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다. 섹션을 참조하세요.

문제 해결

이 문제를 해결하려면 잘못된 헤더 필드를 삭제하도록 로드 밸런서를 구성하세요.

잘못된 헤더 필드를 삭제하도록 로드 밸런서를 구성하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 로드 밸런서를 선택합니다.
3. Application Load Balancer를 선택합니다.
4. 작업에서 속성 편집을 선택합니다.
5. 잘못된 헤더 필드 삭제에서 활성화를 선택합니다.
6. 저장을 선택합니다.

[ELB.5] 애플리케이션 및 Classic Load Balancer 로깅이 활성화되어야 합니다.

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: elb-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Application Load Balancer와 Classic Load Balancer의 로깅이 활성화되었는지 확인합니다. `access_logs.s3.enabled` 이 `false`이면 제어는 실패합니다.

Elastic Load Balancing은 로드 밸런서에 전송된 요청에 대한 자세한 정보를 캡처하는 액세스 로그를 제공합니다. 각 로그에는 요청을 받은 시간, 클라이언트의 IP 주소, 지연 시간, 요청 경로 및 서버 응답과 같은 정보가 포함되어 있습니다. 이러한 액세스 로그를 사용하여 트래픽 패턴을 분석하고 문제를 해결할 수 있습니다.

자세한 정보는 Classic Load Balancer 사용 설명서의 Classic Load Balancer에 대한 액세스 로그를 참조하세요.

문제 해결

액세스 로그를 활성화하려면 Application Load Balancer 사용 설명서의 3단계: 액세스 로그 구성을 참조하세요.

[ELB.6] 애플리케이션, 게이트웨이, Network Load Balancers에는 삭제 보호가 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: elb-deletion-protection-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 애플리케이션, 게이트웨이 또는 Network Load Balancer에 삭제 방지 기능 활성화 여부를 확인합니다. 삭제 방지 기능이 활성화되지 않은 경우, 제어가 실패합니다.

삭제 보호 기능을 활성화하여 애플리케이션, 게이트웨이 또는 Network Load Balancer가 삭제되지 않도록 보호합니다.

문제 해결

로드 밸런서가 실수로 삭제되지 않도록 삭제 방지 기능을 활성화할 수 있습니다. 기본 설정상 로드 밸런서에 대한 삭제 방지 기능은 비활성화되어 있습니다.

로드 밸런서용 삭제 방지 기능을 활성화하는 경우, 로드 밸런서를 삭제하기 전에 삭제 방지를 먼저 비활성화해야 합니다.

Application Load Balancer,에 대한 삭제 방지를 활성화하려면 Application Load Balancer 사용 설명서의 삭제 방지를 참조하세요. 게이트웨이 Load Balancer,에 대한 삭제 방지를 활성화하려면 게이트웨

이 Load Balancer 사용 설명서의 삭제 방지를 참조하세요. Network Load Balancer,에 대한 삭제 방지를 활성화하려면 Network Load Balancer 사용 설명서의 삭제 방지를 참조하세요.

[ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 복구 > 복원력

심각도: 낮음

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: `elb-connection-draining-enabled` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Classic Load Balancer connection draining닝 활성화 여부를 확인합니다.

Classic Load Balancer connection draining닝을 활성화하면 로드 밸런서가 등록 취소 중이거나 비정상 상태인 인스턴스로의 요청 전송을 중지합니다. 이는 기존 연결을 열린 상태로 유지합니다. 이는 Auto Scaling 그룹의 인스턴스에서 연결이 갑자기 끊어지지 않도록 하는 데 특히 유용합니다.

문제 해결

Classic Load Balancer connection draining닝을 활성화하려면 Classic Load Balancer 사용 설명서의 Classic Load Balancer connection draining닝 구성을 참조하세요.

[ELB.8] SSL AWS Config리스너가 있는 Classic Load Balancer는 강력한 요구 사항이 있는 사전 정의된 보안 정책을 사용해야 합니다.

관련 요구 사항: 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 3.13.8, NIST.800-171.r2 3.13.15, PCI DSS v4.0.1/4.2.1

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: elb-predefined-security-policy-ssl-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `predefinedPolicyName`: `ELBSecurityPolicy-TLS-1-2-2017-01`(사용자 지정할 수 없음)

이 제어는 Classic Load Balancer HTTPS/SSL 리스너가 사전 정의된 정책 `ELBSecurityPolicy-TLS-1-2-2017-01`을 사용하는지 여부를 확인합니다. Classic Load Balancer HTTPS/SSL 리스너가 `ELBSecurityPolicy-TLS-1-2-2017-01`을 사용하지 않으면 제어가 실패합니다.

보안 정책은 SSL 프로토콜, 암호 및 서버 순서 기본 설정 옵션의 조합입니다. 사전 정의된 정책은 클라이언트와 로드 밸런서 간의 SSL 협상 동안 지원할 암호, 프로토콜 및 기본 설정 순서를 제어합니다.

`ELBSecurityPolicy-TLS-1-2-2017-01`를 사용하면 특정 버전의 SSL 및 TLS를 비활성화해야 하는 규정 준수 및 보안 표준을 충족하는 데 도움이 됩니다. 자세한 정보는 Classic Load Balancer 사용 설명서의 Classic Load Balancer에 대한 사전 정의된 SSL 보안 정책을 참조하세요.

문제 해결

Classic Load Balancer와 함께 사전 정의된 보안 정책 `ELBSecurityPolicy-TLS-1-2-2017-01`을 사용하는 방법에 대한 자세한 내용은 Classic Load Balancer 사용 설명서의 보안 설정 구성을 참조하세요.

[ELB.9] Classic Load Balancer에는 교차 영역 로드 밸런싱이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: elb-cross-zone-load-balancing-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 CLB(Classic Load Balancer)에 대해 영역 간 로드 밸런싱이 활성화되어 있는지 확인합니다. CLB에 대해 교차 영역 로드 밸런싱이 활성화되어 있지 않은 경우, 제어가 실패합니다.

로드 밸런서 노드는 가용 영역에 등록된 대상에만 트래픽을 분산합니다. 교차 영역 로드 밸런싱을 비활성화하면 각 로드 밸런서 노드가 해당 가용 영역에 있는 등록된 대상 간에만 트래픽을 분산합니다. 등록된 대상의 수가 가용 영역 전체에 동일하지 않으면 트래픽이 균등하게 분산되지 않아 한 영역의 인스턴스가 다른 영역의 인스턴스와 비교하여 과도하게 사용될 수 있습니다. 교차 영역 로드 밸런싱이 활성화되면 Classic Load Balancer에 대한 각각의 로드 밸런서 노드가 활성화된 모든 가용 영역에 있는 등록된 인스턴스 간에 요청을 균등하게 분산합니다. 자세한 내용은 Elastic Load Balancing 사용 설명서의 교차 영역 로드 밸런싱을 참조하세요.

문제 해결

Classic Load Balancer에서 교차 영역 로드 밸런싱을 활성화하려면 Classic Load Balancer 사용 설명서의 교차 영역 로드 밸런싱 활성화를 참조하세요.

[ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: clb-multiple-az

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `minAvailabilityZones` | 최소 가용 영역의 수 | Enum | `2, 3, 4, 5, 6` | 2 |

이 제어는 Classic Load Balancer가 최소한 지정된 수의 가용 영역(AZ)에 걸쳐 구성되었는지 확인합니다. Classic Load Balancer가 최소한 지정된 수의 AZ에 걸쳐 있지 않으면 제어가 실패합니다. 최소 AZs 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 2개의 AZs 사용합니다.

단일 가용 영역 또는 여러 가용 영역의 Amazon EC2 인스턴스에 수신 요청을 분산하도록 Classic Load Balancer를 설정할 수 있습니다. 여러 가용 영역에 걸쳐 있지 않은 Classic Load Balancer는 단독으로 구성된 가용 영역을 사용할 수 없게 되면 트래픽을 다른 가용 영역의 대상으로 리디렉션할 수 없습니다.

문제 해결

Classic Load Balancer에 가용 영역을 추가하려면 Classic Load Balancer 사용 설명서에서 Classic Load Balancer에 대한 서브넷 추가 또는 제거를 참조하세요.

[ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 데이터 무결성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: alb-desync-mode-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `desyncMode`: `defensive, strictest`(사용자 지정할 수 없음)

이 제어는 Application Load Balancer가 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어 있는지 확인합니다. Application Load Balancer가 방어 모드 또는 가장 엄격한 비동기 완화 모드로 구성되지 않은 경우, 제어가 실패합니다.

HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열이나 캐시 중독에 취약해질 수 있습니다. 결과적으로 이러한 취약성으로 인해 보안 인증 정보가 스터핑되거나 승인되지 않은

명령이 실행될 수 있습니다. 방어적 또는 가장 엄격한 비동기화 완화 모드로 구성된 애플리케이션 로드 밸런서는 HTTP 비동기화로 인해 발생할 수 있는 보안 문제로부터 애플리케이션을 보호합니다.

문제 해결

Application Load Balancer의 비동기화 완화 모드를 업데이트하려면 Application Load Balancer 사용 설명서의 비동기화 완화 모드를 참조하세요.

[ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: elbv2-multiple-az

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `minAvailabilityZones` | 최소 가용 영역의 수 | Enum | `2, 3, 4, 5, 6` | `2` |

이 제어는 Elastic Load Balancer V2(애플리케이션, 네트워크 또는 게이트웨이 로드 밸런서)에 최소한 지정된 가용 영역(AZ) 수의 인스턴스가 등록되어 있는지 확인합니다. Elastic Load Balancer V2에 최소한 지정된 AZ 수의 인스턴스가 등록되어 있지 않으면 제어가 실패합니다. 최소 AZs 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 2개의 AZs 사용합니다.

Elastic Load Balancing은 둘 이상의 가용 영역에서 EC2 인스턴스, 컨테이너, IP 주소 등 여러 대상에 걸쳐 수신되는 트래픽을 자동으로 분산합니다. Elastic Load Balancing은 수신 트래픽이 시간이 지남에 따라 변경됨에 따라 로드 밸런서를 확장합니다. Elastic Load Balancer는 하나를 사용할 수 없는 경우,

다른 가용성 영역으로 트래픽을 전달할 수 있으므로 서비스 가용성을 보장하기 위해 최소 두 개의 가용성 영역을 구성하는 것이 좋습니다. 가용 영역을 여러 개 구성하면 애플리케이션에 단일 장애 지점이 발생하는 것을 방지할 수 있습니다.

문제 해결

Application Load Balancer에 가용 영역을 추가하려면 Application Load Balancer 사용 설명서의 Application Load Balancer의 가용 영역을 참조하세요. Network Load Balancer에 가용 영역을 추가하려면 네트워크 로드 밸런서 사용 설명서의 Network Load Balancer 를 참조하세요. 게이트웨이 로드 밸런서에 가용 영역을 추가하려면 게이트웨이 로드 밸런서 사용 설명서의 게이트웨이 로드 밸런서 생성을 참조하세요.

[ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 데이터 무결성

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancing::LoadBalancer`

AWS Config 규칙: clb-desync-mode-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `desyncMode`: `defensive, strictest`(사용자 지정할 수 없음)

이 제어는 Classic Load Balancer가 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어 있는지 확인합니다. Classic Load Balancer가 방어 모드 또는 가장 엄격한 비동기 완화 모드로 구성되지 않은 경우, 제어가 실패합니다.

HTTP 비동기화 문제로 인해 요청 밀수가 발생하고 애플리케이션이 요청 대기열이나 캐시 중독에 취약해질 수 있습니다. 결과적으로 이러한 취약성으로 인해 보안 인증이 도용되거나 승인되지 않은 명령이 실행될 수 있습니다. 방어적이거나 가장 엄격한 비동기화 완화 모드로 구성된 Classic Load Balancer는 HTTP 비동기화로 인해 발생할 수 있는 보안 문제로부터 애플리케이션을 보호합니다.

문제 해결

Classic Load Balancer에서 비동기화 완화 모드를 업데이트하려면 Classic Load Balancer 사용 설명서의 비동기화 완화 모드 수정을 참조하세요.

[ELB.16] Application Load Balancer는 AWS WAF 웹 ACL과 연결되어야 합니다.

관련 요구 사항: NIST.800-53.r5 AC-4(21)

범주: 보호 > 보호 서비스

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::LoadBalancer`

AWS Config 규칙: alb-waf-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Application Load Balancer가 AWS WAF Classic 또는 AWS WAF 웹 액세스 제어 목록(웹 ACL)과 연결되어 있는지 확인합니다. AWS WAF 구성의 `Enabled` 필드가 로 설정된 경우 제어가 실패합니다`false`.

AWS WAF 는 웹 애플리케이션 및 APIs으로부터 보호하는 데 도움이 되는 웹 애플리케이션 방화벽입니다. 를 사용하면 정의한 사용자 지정 가능한 웹 보안 규칙 및 조건을 기반으로 웹 요청을 허용, 차단 또는 계산하는 규칙 세트인 웹 ACL을 구성할 AWS WAF수 있습니다. Application Load Balancer를 AWS WAF 웹 ACL과 연결하여 악의적인 공격으로부터 보호하는 것이 좋습니다.

문제 해결

Application Load Balancer를 웹 ACL과 연결하려면 AWS WAF 개발자 안내서의 웹 ACL을 AWS 리소스와 연결 또는 연결 해제를 참조하세요.

[ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::Listener`

AWS Config 규칙: elbv2-predefined-security-policy-ssl-check

스케줄 유형: 변경이 트리거됨

파라미터: `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`(사용자 지정할 수 없음)

이 제어는 Application Load Balancer의 HTTPS 리스너 또는 Network Load Balancer의 TLS 리스너가 권장 보안 정책을 사용하여 전송 중 데이터를 암호화하도록 구성되어 있는지 확인합니다. 로드 밸런서의 HTTPS 또는 TLS 리스너가 권장 보안 정책을 사용하도록 구성되지 않은 경우 제어가 실패합니다.

Elastic Load Balancing은 보안 정책이라고 하는 SSL 협상 구성을 사용해 클라이언트와 로드 밸런서 간 연결을 협상합니다. 보안 정책은 프로토콜과 암호의 조합을 지정합니다. 프로토콜은 클라이언트와 서버 간에 보안 연결을 설정합니다. 암호는 코딩된 메시지를 생성하기 위해 암호화 키를 사용하는 암호화 알고리즘입니다. 연결 협상이 이루어지는 동안 클라이언트와 로드 밸런서는 각각이 지원하는 암호 및 프로토콜 목록을 선호도 순으로 표시합니다. 로드 밸런서에 권장 보안 정책을 사용하면 규정 준수 및 보안 표준을 충족하는 데 도움이 될 수 있습니다.

문제 해결

권장 보안 정책 및 리스너 업데이트 방법에 대한 자세한 내용은 Elastic Load Balancing 사용 설명서에서 Application Load Balancer에 대한 보안 정책, Network Load Balancer에 대한 보안 정책, Application Load Balancer용 HTTPS 리스너 업데이트, Network Load Balancer용 리스너 업데이트를 참조하세요.

[ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::Listener`

AWS Config 규칙: elbv2-listener-encryption-in-transit

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Application Load Balancer 또는 Network Load Balancer의 리스너가 전송 중 데이터 암호화에 보안 프로토콜을 사용하도록 구성되어 있는지 확인합니다. Application Load Balancer 리스너가 HTTPS 프로토콜을 사용하도록 구성되지 않았거나 Network Load Balancer 리스너가 TLS 프로토콜을 사용하도록 구성되지 않은 경우 제어가 실패합니다.

클라이언트와 로드 밸런서 간에 전송되는 데이터를 암호화하려면 HTTPS(Application Load Balancer의 경우) 또는 TLS(Network Load Balancer의 경우)와 같은 업계 표준 보안 프로토콜을 사용하도록 Elastic Load Balancer 리스너를 구성해야 합니다. 그렇지 않으면 클라이언트와 로드 밸런서 간에 전송되는 데이터가 가로채기, 변조, 무단 액세스에 취약합니다. 리스너에서 HTTPS 또는 TLS 사용은 보안 모범 사례에 부합하며 전송 중 데이터의 기밀성 및 무결성을 보장하는 데 도움이 됩니다. 이는 민감한 정보를 처리하는 애플리케이션 또는 전송 중 데이터 암호화를 요구하는 보안 표준을 준수해야 하는 애플리케이션에 특히 중요합니다.

문제 해결

리스너에 대해 보안 프로토콜을 구성하는 방법에 대한 자세한 내용은 Elastic Load Balancing 사용 설명서의 Application Load Balancer용 HTTPS 리스너 생성 및 Network Load Balancer용 리스너 생성을 참조하세요.

[ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config 규칙: elbv2-targetgroup-healthcheck-protocol-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 애플리케이션 및 네트워크 로드 밸런서 상태 확인을 위한 대상 그룹이 암호화된 전송 프로토콜을 사용하는지 여부를 확인합니다. 상태 확인 프로토콜이 HTTPS를 사용하지 않으면 제어가 실패합니다. 이 제어는 Lambda 대상 유형에 적용되지 않습니다.

로드 밸런서는 등록된 대상에 상태 확인 요청을 보내 상태를 확인하고 그에 따라 트래픽을 라우팅합니다. 대상 그룹 구성에 지정된 상태 확인 프로토콜에 따라 이러한 검사가 수행되는 방식이 결정됩니다. 상태 확인 프로토콜이 HTTP와 같은 암호화되지 않은 통신을 사용하는 경우 전송 중에 요청 및 응답을 가로채거나 조작할 수 있습니다. 이를 통해 공격자는 인프라 구성에 대한 인사이트를 얻거나, 상태 확인 결과를 변조하거나, 라우팅 결정에 영향을 미치는 man-in-the-middle 공격을 수행할 수 있습니다. 상태 확인에 HTTPS를 사용하면 로드 밸런서와 대상 간에 암호화된 통신을 제공하여 상태 정보의 무결성과 기밀성을 보호할 수 있습니다.

문제 해결

Application Load Balancer 대상 그룹에 대해 암호화된 상태 확인을 구성하려면 Elastic Load Balancing 사용 설명서의 Application Load Balancer 대상 그룹의 상태 확인 설정 업데이트를 참조하세요. Network Load Balancer 대상 그룹에 대해 암호화된 상태 확인을 구성하려면 Elastic Load Balancing 사용 설명서의 Network Load Balancer 대상 그룹의 상태 확인 설정 업데이트를 참조하세요.

[ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::ElasticLoadBalancingV2::TargetGroup`

AWS Config 규칙: elbv2-targetgroup-protocol-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Elastic Load Balancing 대상 그룹이 암호화된 전송 프로토콜을 사용하는지 확인합니다. 이 제어는 대상 유형이 Lambda 또는 ALB인 대상 그룹 또는 GENEVE 프로토콜을 사용하는 대상 그룹에는 적용되지 않습니다. 대상 그룹이 HTTPS, TLS 또는 QUIC 프로토콜을 사용하지 않으면 제어가 실패합니다.

전송 중 데이터를 암호화하면 권한이 없는 사용자의 가로채기로부터 데이터를 보호할 수 있습니다. 암호화되지 않은 프로토콜(HTTP, TCP, UDP)을 사용하는 대상 그룹은 암호화 없이 데이터를 전송하므로

도청에 취약합니다. 암호화된 프로토콜(HTTPS, TLS, QUIC)을 사용하면 로드 밸런서와 대상 간에 전송되는 데이터를 보호할 수 있습니다.

문제 해결

암호화된 프로토콜을 사용하려면 HTTPS, TLS 또는 QUIC 프로토콜을 사용하여 새 대상 그룹을 생성해야 합니다. 생성 후에는 대상 그룹 프로토콜을 수정할 수 없습니다. Application Load Balancer 대상 그룹을 생성하려면 Elastic Load Balancing 사용 설명서의 Application Load Balancer의 대상 그룹 생성을 참조하세요. Network Load Balancer 대상 그룹을 생성하려면 Elastic Load Balancing 사용 설명서의 Network Load Balancer에 대한 대상 그룹 생성을 참조하세요.

## Elasticsearch용 Security Hub CSPM

이러한 AWS Security Hub CSPM 제어는 Elasticsearch 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-encrypted-at-rest`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Elasticsearch 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다.

OpenSearch의 민감한 데이터에 대한 보안 계층을 추가하려면 저장 시 OpenSearch를 암호화하도록 구성해야 합니다. Elasticsearch 도메인은 저장 데이터 암호화를 제공합니다. 이 기능은 AWS KMS 를 사용하여 암호화 키를 저장하고 관리합니다. 암호화를 수행하기 위해 256비트 키(AES-256)가 있는 고급 암호화 표준 알고리즘을 사용합니다.

OpenSearch 저장 시 암호화에 대해 자세히 알아보려면 Amazon OpenSearch Service 개발자 안내서의 Amazon OpenSearch Service에 대한 저장 데이터 암호화를 참조하세요.

`t.small` 및 `t.medium` 등의 특정 인스턴스 유형은 저장 데이터의 암호화를 지원하지 않습니다. 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 지원되는 인스턴스 유형을 참조하세요.

문제 해결

새로운 및 기존 Elasticsearch 도메인에 대해 저장 시 암호화를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 저장 데이터 암호화 활성화를 참조하세요.

[ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 심각

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-in-vpc-only`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Elasticsearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. Elasticsearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. Amazon OpenSearch Service 개발자 안내서의 리소스 기반 정책을 참조하세요. 또한 권장 모범 사례에 따라 VPC가 구성되었는지 확인해야 합니다. 또한 Amazon VPC 사용 설명서에서 VPC에 대한 보안 모범 사례를 참조하세요.

VPC 내에 배포된 Elasticsearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS 네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPC는 네트워크 ACL 및 보안 그룹을 포함하여 Elasticsearch 도메인에 대한 액세

스를 보호하기 위한 여러 네트워크 제어를 제공합니다. Security Hub CSPM은 이러한 제어를 활용하기 위해 퍼블릭 Elasticsearch 도메인을 VPCs로 마이그레이션할 것을 권장합니다.

문제 해결

퍼블릭 엔드포인트가 있는 도메인을 만들 경우, 나중에 해당 도메인을 VPC 안에 배치할 수 없습니다. 대신에 새로운 도메인을 만들어 데이터를 마이그레이션해야 합니다. 반대의 경우도 마찬가지입니다. VPC 내에 도메인을 만들 경우, 퍼블릭 엔드포인트를 가질 수 없습니다. 대신 다른 도메인을 만들거나 이 제어를 비활성화해야 합니다.

Amazon OpenSearch Service 개발자 안내서의 VPC 내에서 Amazon OpenSearch Service 도메인 시작을 참조하세요.

[ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-node-to-node-encryption-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Elasticsearch 도메인에 노드 간 암호화가 활성화되어 있는지 확인합니다. Elasticsearch 도메인에 노드 간 암호화가 활성화되어 있지 않은 경우, 제어가 실패합니다. 또한 Elasticsearch 버전이 노드 간 암호화 검사를 지원하지 않는 경우에도 제어는 실패한 조사 결과를 생성합니다.

HTTPS(TLS)를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 통해 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. Elasticsearch 도메인의 노드 간 암호화를 활성화하면 클러스터 내 통신이 전송 중 암호화됩니다.

이 구성과 관련하여 성능이 저하될 수 있습니다. 이 옵션을 활성화하기 전에 성능 균형을 파악하고 테스트해야 합니다.

문제 해결

새로운 및 기존 도메인에서 노드 간 암호화 활성화에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 노드 간 암호화 활성화를 참조하세요.

[ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.

관련 요구 사항: 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)

범주: 식별 - 로깅

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-logs-to-cloudwatch`

스케줄 유형: 변경이 트리거됨

파라미터:

- `logtype = 'error'`(사용자 지정할 수 없음)

이 제어는 Elasticsearch 도메인이 오류 로그를 CloudWatch Logs로 전송하도록 구성되었는지 여부를 확인합니다.

Elasticsearch 도메인의 오류 로그를 활성화하고 해당 로그를 CloudWatch Logs로 전송하여 보존 및 응답을 받아야 합니다. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

문제 해결

로그 게시를 활성화하는 방법에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 로그 게시 활성화(콘솔)를 참조하세요.

[ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-audit-logging-enabled` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

- `cloudWatchLogsLogGroupArnList`(사용자 지정할 수 없음). Security Hub CSPM은이 파라미터를 채우지 않습니다. 감사 로그용으로 구성해야 하는 CloudWatch Logs 로그 그룹을 쉼표로 구분한 목록입니다.

  이 규칙 `NON_COMPLIANT`은 Elasticsearch 도메인의 CloudWatch Logs 로그 그룹이 이 파라미터 목록에 지정되지 않은 경우입니다.

이 제어는 Elasticsearch 도메인에 감사 로깅이 활성화되어 있는지 여부를 확인합니다. Elasticsearch 도메인에 감사 로깅이 활성화되어 있지 않으면 이 제어가 실패합니다.

감사 로그는 고도로 사용자 지정이 가능합니다. 이를 통해 인증 성공 및 실패, OpenSearch 요청, 인덱스 변경, 수신 검색 쿼리 등 Elasticsearch 클러스터에서 사용자 활동을 추적할 수 있습니다.

문제 해결

감사 로그 활성화에 대한 자세한 지침은 Amazon OpenSearch Service 개발자 안내서의 감사 로그 활성화를 참조하세요.

[ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-data-node-fault-tolerance` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Elasticsearch 도메인이 최소 세 개의 데이터 노드로 구성되어 있고 `zoneAwarenessEnabled`이 `true`인지 확인합니다.

Elasticsearch 도메인에는 고가용성 및 내결함성을 위해 최소 3개의 데이터 노드가 필요합니다. 최소 3개의 데이터 노드가 있는 Elasticsearch 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.

문제 해결

Elasticsearch 도메인의 데이터 노드 수를 수정하려면

1. https://console.aws.amazon.com/aos/ Amazon OpenSearch Service 콘솔을 엽니다.
2. 도메인에서 편집하려는 도메인의 이름을 선택합니다.
3. 도메인 편집을 선택합니다.
4. 데이터 노드에서 노드 수를 3 이상의 수로 설정합니다.

   3개의 가용 영역 배포의 경우, 가용 영역 전체에 균등하게 배포되도록 3의 배수로 설정합니다.
5. 제출을 선택합니다.

[ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config규칙: `elasticsearch-primary-node-fault-tolerance` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Elasticsearch 도메인이 최소 3개의 전용 프라이머리 노드로 구성되어 있는지 확인합니다. 도메인이 전용 프라이머리 노드를 사용하지 않는 경우, 이 제어는 실패합니다. Elasticsearch 도메인에 5개의 전용 프라이머리 노드가 있는 경우, 이 제어는 통과됩니다. 그러나 가용성 위험을 완화하기 위해 3개 이상의 프라이머리 노드를 사용하는 것은 불필요할 수 있으며 추가 비용이 발생합니다.

Elasticsearch 도메인에는 고가용성 및 내결함성을 위해 최소 3개의 전용 프라이머리 노드가 필요합니다. 관리해야 할 추가 노드가 있기 때문에 데이터 노드 블루/그린 배포 중에 전용 프라이머리 노드 리소스가 부족해질 수 있습니다. 3개 이상의 전용 프라이머리 노드가 포함된 Elasticsearch 도메인을 배포하면 노드 장애 시 충분한 프라이머리 노드 리소스 용량과 클러스터 운영이 보장됩니다.

문제 해결

OpenSearch 도메인의 전용 프라이머리 노드 수를 수정하려면

1. https://console.aws.amazon.com/aos/ Amazon OpenSearch Service 콘솔을 엽니다.
2. 도메인에서 편집하려는 도메인의 이름을 선택합니다.
3. 도메인 편집을 선택합니다.
4. 전용 프라이머리 노드에서 인스턴스 유형을 원하는 인스턴스 유형으로 설정합니다.
5. 프라이머리 노드 수를 3개 이상으로 설정합니다.
6. 제출을 선택합니다.

[ES.8] Elasticsearch 도메인에 대한 연결은 TLS 보안 정책을 사용하여 암호화해야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `elasticsearch-https-required` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Elasticsearch 도메인 엔드포인트가 최신 TLS 보안 정책을 사용하도록 구성되어 있는지 확인합니다. Elasticsearch 도메인 엔드포인트가 지원되는 최신 정책을 사용하도록 구성되지 않았거나 HTTP가 활성화되어 있지 않은 경우, 제어가 실패합니다. 현재 지원되는 최신 TLS 보안 정책은 `Policy-Min-TLS-1-2-PFS-2023-10`입니다.

HTTPS(TLS)를 사용하여 잠재적 공격자가 중간자 또는 그와 유사한 공격을 사용하여 네트워크 트래픽을 염탐하거나 조작하지 못하게 할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다. TLS 1.2는 이전 버전의 TLS보다 몇 가지 향상된 보안 기능을 제공합니다.

문제 해결

TLS 암호화를 활성화하려면 을 설정하기 위해 UpdateDomainConfig API 작업을 사용하여 DomainEndpointOptions 객체를 구성합니다. 이렇게 하면 `TLSSecurityPolicy`이 설정됩니다.

[ES.9] Elasticsearch 도메인에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Elasticsearch::Domain`

AWS Config 규칙: `tagged-elasticsearch-domain` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Elasticsearch 도메인에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 도메인에 태그 키가 없거나 파라미터 `requiredTagKeys`에 모든 키가 지정되지 않은 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이(가) 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 도메인에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Elasticsearch 도메인에 태그를 추가하려면 Amazon OpenSearch Service 개발자 안내서의 태그 작업을 참조하세요.

## Amazon EMR에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon EMR(이전 Amazon Elastic MapReduce) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::EMR::Cluster`

AWS Config규칙: emr-master-no-public-ip

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EMR 클러스터의 프라이머리 노드에 퍼블릭 IP 주소가 있는지 확인합니다. 퍼블릭 IP 주소가 프라이머리 노드 인스턴스 중 하나와 연결되어 있는 경우, 제어가 실패합니다.

퍼블릭 IP 주소는 인스턴스에 대한 `NetworkInterfaces` 구성의 `PublicIp` 필드에 지정됩니다. 이 제어는 `RUNNING` 또는 `WAITING` 상태에 있는 Amazon EMR 클러스터만 검사합니다.

문제 해결

시작하는 동안 기본 또는 기본이 아닌 서브넷의 인스턴스에 퍼블릭 IPv4 주소를 할당할지 여부를 제어할 수 있습니다. 기본적으로 기본 서브넷의 속성 값은 `true`로 설정되어 있습니다. 기본이 아닌 서브넷은 Amazon EC2 시작 인스턴스 마법사로 생성되지 않은 한 IPv4 퍼블릭 주소 지정 속성이 `false`로 설정되어 있습니다. 이 경우, 속성이 `true`로 설정됩니다.

시작 후에는 인스턴스에서 퍼블릭 IPv4 주소를 수동으로 연결 해제할 수 없습니다.

실패한 조사 결과를 수정하려면 IPv4 퍼블릭 주소 지정 속성이 `false`으로 설정된 프라이빗 서브넷이 있는 VPC에서 새로운 클러스터를 시작해야 합니다. 지침은 Amazon EMR 관리 안내서의 VPC로 클러스터 시작을 참조하세요.

[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config규칙: emr-block-public-access

스케줄 유형: 주기적

파라미터: 없음

이 제어는 계정이 Amazon EMR 퍼블릭 액세스 차단을 사용하여 구성되어 있는지 확인합니다. 퍼블릭 액세스 차단 설정이 활성화되지 않았거나 포트 22가 아닌 다른 포트가 허용되면 제어가 실패합니다.

Amazon EMR 퍼블릭 액세스 차단을 사용하면 클러스터에 포트의 퍼블릭 IP 주소로부터 들어오는 인바운드 트래픽을 허용하는 보안 구성이 있는 경우, 퍼블릭 서브넷에서 클러스터를 시작할 수 없습니다. AWS 계정의 사용자가 클러스터를 시작하면 Amazon EMR은 클러스터의 보안 그룹에서 포트 규칙을 확인하고 이를 인바운드 트래픽 규칙과 비교합니다. 보안 그룹에 퍼블릭 IP 주소 IPv4 0.0.0.0/0 또는 IPv6: :/0에 대해 포트를 여는 인바운드 규칙이 있고 해당 포트가 계정에 대한 예외로 지정되지 않은 경우, Amazon EMR은 사용자의 클러스터 생성을 허용하지 않습니다.

> **Note**
>
> 퍼블릭 액세스 차단은 기본적으로 활성화되어 있습니다. 계정 보호를 강화하려면 이 기능을 활성화된 상태로 유지하는 것이 좋습니다.

문제 해결

Amazon EMR에 대한 퍼블릭 액세스 차단을 구성하려면 Amazon EMR 관리 가이드의 Amazon EMR 블록 퍼블릭 액세스 사용을 참조하세요.

[EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CP-9(8), NIST.800-53.r5 SI-12

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EMR::SecurityConfiguration`

AWS Config 규칙: emr-security-configuration-encryption-rest

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EMR 보안 구성에 저장 시 암호화가 활성화되어 있는지 확인합니다. 보안 구성이 저장 시 암호화를 활성화하지 않는 경우 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 저장 데이터를 암호화하면 기밀성을 보호할 수 있으므로 권한이 없는 사용자가 데이터에 액세스할 수 있는 위험이 줄어듭니다.

문제 해결

Amazon EMR 보안 구성에서 저장 시 암호화를 활성화하려면 Amazon EMR 관리 안내서의 데이터 암호화 구성을 참조하세요.

[EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::EMR::SecurityConfiguration`

AWS Config 규칙: emr-security-configuration-encryption-transit

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EMR 보안 구성에 전송 중 암호화가 활성화되어 있는지 확인합니다. 보안 구성이 전송 중 암호화를 활성화하지 않는 경우 제어가 실패합니다.

전송 중 데이터는 클러스터의 노드 사이 또는 클러스터와 애플리케이션 사이와 같이 한 위치에서 다른 위치로 이동하는 데이터를 나타냅니다. 데이터는 인터넷 또는 프라이빗 네트워크 내에서 이동할 수 있

습니다. 전송 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다.

문제 해결

Amazon EMR 보안 구성에서 전송 중 암호화를 활성화하려면 Amazon EMR 관리 안내서의 데이터 암호화 구성을 참조하세요.

## EventBridge에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon EventBridge 서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Events::EventBus`

AWS Config규칙:`tagged-events-eventbus` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon EventBridge 이벤트 버스에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 이벤트 버스에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정

된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 이벤트 버스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

EventBridge 이벤트 버스에 태그를 추가하려면 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하세요.

[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 낮음

리소스 유형: `AWS::Events::EventBus`

AWS Config 규칙: custom-eventbus-policy-attached

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EventBridge 사용자 지정 이벤트 버스에 리소스 기반 정책이 연결되어 있는지 확인합니다. 사용자 지정 이벤트 버스에 리소스 기반 정책이 없는 경우, 이 제어가 실패합니다.

기본적으로 EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있지 않습니다. 이렇게 하면 계정의 보안 주체가 이벤트 버스에 액세스할 수 있습니다. 이벤트 버스에 리소스 기반 정책을 연결하면 이벤트 버스에 대한 액세스를 지정된 계정으로 제한할 수 있을 뿐만 아니라 의도적으로 다른 계정의 엔터티에 대한 액세스 권한을 부여할 수도 있습니다.

문제 해결

EventBridge 사용자 지정 이벤트 버스에 리소스 기반 정책을 연결하려면 Amazon EventBridge 사용 설명서의 이벤트 버스 권한 관리를 참조하세요.

[EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Events::Endpoint`

AWS Config 규칙: `global-endpoint-event-replication-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon EventBridge 글로벌 엔드포인트에 대해 이벤트 복제가 활성화되어 있는지 확인합니다. 글로벌 엔드포인트에서 이벤트 복제가 활성화되지 않은 경우, 제어가 실패합니다.

글로벌 엔드포인트는 애플리케이션의 리전별 내결함성을 높이는 데 도움이 됩니다. 시작하려면 Amazon Route 53 상태 확인을 엔드포인트에 할당합니다. 장애 조치가 시작되면 상태 확인에서 "비정상" 상태를 보고합니다. 장애 조치가 시작된 후 몇 분 이내에 모든 사용자 지정 이벤트는 보조 리전의 이벤트 버스로 라우팅되고 해당 이벤트 버스에 의해 처리됩니다. 글로벌 엔드포인트를 사용하면 이벤

트 복제를 활성화할 수 있습니다. 이벤트 복제는 관리형 규칙을 사용하여 모든 사용자 지정 이벤트를 기본 및 보조 리전의 이벤트 버스로 전송합니다. 글로벌 엔드포인트를 설정할 때는 이벤트 복제를 활성화하는 것이 좋습니다. 이벤트 복제를 통해 글로벌 엔드포인트가 올바르게 구성되었는지 확인할 수 있습니다. 장애 조치 이벤트에서 자동으로 복구하려면 이벤트 복제가 필요합니다. 이벤트 복제를 활성화하지 않은 경우, 이벤트가 기본 리전으로 다시 라우팅되기 전에 Route 53 상태 확인을 "정상"으로 수동으로 재설정해야 합니다.

> **Note**
>
> 사용자 지정 이벤트 버스를 사용하는 경우, 장애 조치가 제대로 작동하려면 각 리전에 동일한 이름과 동일한 계정을 가진 사용자 정의 짝수 버스가 필요합니다. 이벤트 복제를 활성화하면 월별 비용이 증가할 수 있습니다. 요금에 대한 자세한 내용은 Amazon EventBridge 요금을 참조하세요.

문제 해결

EventBridge 글로벌 엔드포인트에 대한 이벤트 복제를 활성화하려면 Amazon EventBridge 사용 설명서의 글로벌 엔드포인트 생성을 참조하세요. 이벤트 복제의 경우, 이벤트 복제 활성화를 선택합니다.

## Amazon Fraud Detector에 대한 Security Hub CSPM 제어

이러한 Security Hub CSPM 제어는 Amazon Fraud Detector 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::FraudDetector::EntityType`

AWS Config 규칙: `frauddetector-entity-type-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| requiredKeyTags | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Fraud Detector 엔터티 유형에 파라미터 requiredKeyTags에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 엔터티 유형에 태그 키가 없거나 파라미터 requiredKeyTags에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 requiredKeyTags가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 엔터티 유형에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

Amazon Fraud Detector 엔터티 유형에 태그를 추가하려면(콘솔)

1. https://console.aws.amazon.com/frauddetector에서 Amazon Fraud Detector 콘솔을 엽니다.
2. 탐색 창에서 엔터티를 선택합니다.

3. 목록에서 엔터티 유형을 선택합니다.
4. 엔터티 유형 태그 섹션에서 태그 관리를 선택합니다.
5. 새로운 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 페어에 대해 반복합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

[FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::FraudDetector::Label`

AWS Config 규칙: `frauddetector-label-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Fraud Detector 레이블에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 레이블에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 레이블에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는

데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

Amazon Fraud Detector 레이블에 태그를 추가하려면(콘솔)

1. https://console.aws.amazon.com/frauddetector에서 Amazon Fraud Detector 콘솔을 엽니다.
2. 탐색 창에서 레이블을 선택합니다.
3. 목록에서 레이블을 선택합니다.
4. 레이블 태그 섹션에서 태그 관리를 선택합니다.
5. 새로운 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 페어에 대해 반복합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

[FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::FraudDetector::Outcome`

AWS Config 규칙: `frauddetector-outcome-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Fraud Detector 결과에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 결과에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 결과에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

Amazon Fraud Detector 결과에 태그를 추가하려면(콘솔)

1. https://console.aws.amazon.com/frauddetector에서 Amazon Fraud Detector 콘솔을 엽니다.
2. 탐색 창에서 결과를 선택합니다.

3. 목록에서 결과를 선택합니다.
4. 결과 태그 섹션에서 태그 관리를 선택합니다.
5. 새로운 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 페어에 대해 반복합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

[FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::FraudDetector::Variable`

AWS Config 규칙: `frauddetector-variable-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Fraud Detector 변수에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 변수에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 변수에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는

데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

Amazon Fraud Detector 변수에 태그를 추가하려면(콘솔)

1. https://console.aws.amazon.com/frauddetector에서 Amazon Fraud Detector 콘솔을 엽니다.
2. 탐색 창에서 변수를 선택합니다.
3. 목록에서 변수를 선택합니다.
4. 변수 태그 섹션에서 태그 관리를 선택합니다.
5. 새로운 태그 추가를 선택합니다. 해당 태그의 키와 값을 입력합니다. 추가 키-값 페어에 대해 반복합니다.
6. 태그 추가가 완료되면 저장을 선택합니다.

## Amazon FSx에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon FSx 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::FSx::FileSystem`

AWS Config 규칙: fsx-openzfs-copy-tags-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있는지 확인합니다. OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되지 않은 경우, 제어가 실패합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 태그를 사용하면 용도, 소유자 또는 환경 등 다양한 방식으로 AWS리소스를 분류할 수 있습니다. 이 기능은 동일 유형의 리소스가 많을 때 유용합니다. 지정한 태그에 따라 특정 리소스를 빠르게 식별할 수 있기 때문입니다.

문제 해결

백업 및 볼륨에 태그를 복사하도록 FSx for OpenZFS 파일 시스템을 구성하는 방법에 대한 자세한 내용은 Amazon FSx for OpenZFS 사용 설명서의 파일 시스템 업데이트를 참조하세요.

[FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-9, NIST.800-53.r5 CM-8

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::FSx::FileSystem`

AWS Config 규칙: fsx-lustre-copy-tags-to-backups

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon FSx for Lustre 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있는지 확인합니다. Lustre 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되지 않은 경우, 제어가 실패합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 태그를 사용하면 용도, 소유자 또는 환경 등 다양한 방식으로 AWS리소스를 분류할 수 있습니다. 이 기능은 동일 유형의 리소스가 많을 때 유용합니다. 지정한 태그에 따라 특정 리소스를 빠르게 식별할 수 있기 때문입니다.

문제 해결

백업에 태그를 복사하도록 FSx for Lustre 파일 시스템을 구성하는 방법에 대한 자세한 내용은 Amazon FSx for Lustre 사용 설명서의 동일한 AWS 계정 내에서 백업 복사를 참조하세요.

[FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::FSx::FileSystem`

AWS Config 규칙: fsx-openzfs-deployment-type-check

스케줄 유형: 주기적

파라미터: `deploymentTypes: MULTI_AZ_1`(사용자 지정할 수 없음)

이 제어는 Amazon FSx for OpenZFS 파일 시스템이 다중 가용 영역(다중 AZ) 배포 유형을 사용하도록 구성되어 있는지 확인합니다. 파일 시스템이 다중 AZ 배포 유형을 사용하도록 구성되지 않은 경우 제어가 실패합니다.

Amazon FSx for OpenZFS는 파일 시스템에 다중 AZ(HA), 단일 AZ(HA) 및 단일 AZ(비 HA) 배포 유형을 지원합니다. 각 배포 유형은 다양한 수준의 가용성 및 내구성을 제공합니다. 다중 AZ(HA) 파일 시스템은 2개의 가용 영역(AZ)에 분산된 한 쌍의 고가용성(HA) 파일 서버로 구성됩니다. 대부분의 프로덕션 워크로드에는 고가용성 및 내구성 모델을 제공하는 다중 AZ(HA) 배포 유형을 사용하는 것이 좋습니다.

문제 해결

파일 시스템을 생성할 때 다중 AZ 배포 유형을 사용하도록 Amazon FSx for OpenZFS 파일 시스템을 구성할 수 있습니다. 기존 FSx for OpenZFS 파일 시스템의 배포 유형은 변경할 수 없습니다.

FSx for OpenZFS 파일 시스템의 배포 유형 및 옵션에 대한 자세한 내용은 Amazon FSx for OpenZFS 사용 설명서의 Amazon FSx for OpenZFS의 가용성 및 내구성 및 파일 시스템 리소스 관리를 참조하세요.

[FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::FSx::FileSystem`

AWS Config 규칙: fsx-ontap-deployment-type-check

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `deploymentTypes` | 평가에 포함할 배포 유형의 목록입니다. 파일 시스템이 목록에 지정된 배포 유형을 사용하도록 구성되지 않은 경우 제어는 `FAILED` 조사 결과를 생성합니다. | Enum | `MULTI_AZ_1` , `MULTI_AZ_2` | `MULTI_AZ_1` , `MULTI_AZ_2` |

이 제어는 Amazon FSx for NetApp ONTAP 파일 시스템이 다중 가용 영역(다중 AZ) 배포 유형을 사용하도록 구성되어 있는지 확인합니다. 파일 시스템이 다중 AZ 배포 유형을 사용하도록 구성되지 않은 경우 제어가 실패합니다. 선택적으로 평가에 포함할 배포 유형의 목록을 지정할 수 있습니다.

Amazon FSx for NetApp ONTAP은 파일 시스템에 단일 AZ 1, 단일 AZ 2, 다중 AZ 1 및 다중 AZ 2 배포 유형을 지원합니다. 각 배포 유형은 다양한 수준의 가용성 및 내구성을 제공합니다. 대부분의 프로덕션 워크로드에는 고가용성 및 내구성 모델을 제공하는 다중 AZ 배포 유형을 사용하는 것이 좋습니다. 다중 AZ 파일 시스템은 Single-AZ 파일 시스템의 가용성 및 내구성 기능을 모두 지원합니다. 또한 가용 영역(AZ)을 사용할 수 없는 경우에도 지속적인 데이터 가용성을 제공하도록 설계되었습니다.

문제 해결

기존 Amazon FSx for NetApp ONTAP 파일 시스템의 배포 유형은 변경할 수 없습니다. 그러나 데이터를 백업하고 다중 AZ 배포 유형을 사용하는 새 파일 시스템에서 복원할 수 있습니다.

FSx for ONTAP 파일 시스템의 배포 유형 및 옵션에 대한 자세한 내용은 FSx for ONTAP 사용 설명서의 가용성, 내구성 및 배포 옵션 및 파일 시스템 관리를 참조하세요.

[FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::FSx::FileSystem`

AWS Config 규칙: fsx-windows-deployment-type-check

스케줄 유형: 주기적

파라미터: `deploymentTypes: MULTI_AZ_1`(사용자 지정할 수 없음)

이 제어는 Amazon FSx for Windows File Server 파일 시스템이 다중 가용 영역(다중 AZ) 배포 유형을 사용하도록 구성되어 있는지 확인합니다. 파일 시스템이 다중 AZ 배포 유형을 사용하도록 구성되지 않은 경우 제어가 실패합니다.

Amazon FSx for Windows File Server는 파일 시스템에 단일 AZ 및 다중 AZ 배포 유형을 지원합니다. 각 배포 유형은 다양한 수준의 가용성 및 내구성을 제공합니다. 단일 AZ 파일 시스템은 단일 Windows 파일 서버 인스턴스와, 단일 가용 영역 내의 스토리지 볼륨 세트로 구성됩니다. 다중 AZ 파일 시스템은 2개의 가용 영역에 분산된 Windows 파일 서버 고가용성 클러스터로 구성됩니다. 대부분의 프로덕션 워크로드에는 고가용성 및 내구성 모델을 제공하는 다중 AZ 배포 유형을 사용하는 것이 좋습니다.

문제 해결

파일 시스템을 생성할 때 다중 AZ 배포 유형을 사용하도록 Amazon FSx for Windows File Server 파일 시스템을 구성할 수 있습니다. 기존 FSx for Windows File Server 파일 시스템의 배포 유형은 변경할 수 없습니다.

FSx for Windows File Server 파일 시스템의 배포 유형 및 옵션에 대한 자세한 내용은 Amazon FSx for Windows File Server 사용 설명서의 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템 및 Amazon FSx for Windows File Server 시작하기를 참조하세요.

## Global Accelerator에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWS Global Accelerator서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::GlobalAccelerator::Accelerator`

AWS Config규칙: `tagged-globalaccelerator-accelerator` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 액셀러AWS Global Accelerator레이터에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 액셀러레이터에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 액셀러레이터에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Global Accelerator 글로벌 액셀러레이터에 태그를 추가하려면 AWS Global Accelerator 개발자 안내서의 AWS Global Accelerator에서 태그 지정을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Glue

이러한 AWS Security Hub CSPM제어는 AWS Glue서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Glue.1]AWS Glue작업에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Glue::Job`

AWS Config규칙: `tagged-glue-job` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Glue작업에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 작업에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 작업에 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS Glue작업에 태그를 추가하려면 AWS Glue사용 설명서의에서 AWS태그를AWS Glue 참조하세요.

[Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: AWS::Glue::MLTransform

AWS Config 규칙: glue-ml-transform-encrypted-at-rest

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Glue기계 학습 변환이 저장 시 암호화되는지 확인합니다. 기계 학습 변환이 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 저장 데이터를 암호화하면 기밀성을 보호할 수 있으므로 권한이 없는 사용자가 데이터에 액세스할 수 있는 위험이 줄어듭니다.

문제 해결

AWS Glue기계 학습 변환에 대한 암호화를 구성하려면 AWS Glue사용 설명서의 기계 학습 변환 작업을 참조하세요.

[Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue

관련 요구 사항: 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)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::Glue::Job`

AWS Config 규칙: glue-spark-job-supported-version

스케줄 유형: 변경이 트리거됨

파라미터: `minimumSupportedGlueVersion`: `3.0`(사용자 지정할 수 없음)

이 제어는 AWS Gluefor Spark 작업이 지원되는 버전에서 실행되도록 구성되어 있는지 확인합니다 AWS Glue. Spark 작업이 지원되는 최소 버전보다 이전 버전의에서 실행되도록 구성된 경우 제어AWS Glue가 실패합니다.

> **Note**
>
> 또한이 제어는 작업의 구성 항목(CIGlueVersion)에 AWS Glue버전() 속성이 없거나 null인 경우 AWS Gluefor Spark 작업에 대한 `FAILED` 결과를 생성합니다. 이러한 경우 조사 결과에 주석 `GlueVersion is null or missing in glueetl job configuration`이 포함됩니다. 이러한 유형의 `FAILED` 조사 결과를 해결하려면 작업의 구성에 `GlueVersion` 속성을 추가합니다. 지원되는 버전 및 런타임 환경의 목록은 AWS Glue 사용 설명서의 AWS Glue 버전을 참조하세요.

최신 버전의에서 AWS GlueSpark 작업을 실행하면의 성능, 보안 및 최신 기능에 대한 액세스를 최적화할 AWS Glue수 있습니다AWS Glue. 또한 보안 취약성으로부터 보호하는 데 도움이 될 수 있습니다. 예를 들어 보안 업데이트를 제공하거나, 문제를 해결하거나, 새로운 기능을 도입하기 위해 새 버전이 릴리스될 수 있습니다.

문제 해결

Spark 작업을 지원되는 버전으로 마이그레이션하는 방법에 대한 자세한 내용은 AWS Glue사용 설명서의 Spark 작업 마이그레이션을 AWS Glue참조하세요. AWS Glue

## Amazon GuardDuty에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon GuardDuty 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[GuardDuty.1] GuardDuty를 활성화해야 합니다.

관련 요구 사항: 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), NIST.800-53.r5 SI-4(22), NIST.800-53.r5 SI-4(25), NIST.800-53.r5 SI-4(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

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: guardduty-enabled-centralized

스케줄 유형: 주기적

파라미터: 없음

이 제어는 GuardDuty 계정 및 리전에서 Amazon GuardDuty가 활성화되어 있는지 확인합니다.

지원되는 모든 AWS리전에서 GuardDuty를 활성화하는 것이 좋습니다. 이렇게 하면 현재 활발히 사용하고 있지 않은 리전에서도 비정상적인 활동이나 허가되지 않은 활동에 대한 조사 결과를 GuardDuty를 통해 생성할 수 있습니다. 또한 이를 통해 GuardDuty는 IAM과 같은 글로벌 AWS 서비스에 대한 CloudTrail 이벤트를 모니터링할 수 있습니다.

문제 해결

GuardDuty 활성화하려면 Amazon GuardDuty 사용 설명서의 GuardDuty 시작을 참조하세요.

[GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::GuardDuty::Filter`

AWS Config규칙: `tagged-guardduty-filter` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon GuardDuty 필터에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 필터에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 필터에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검

색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

GuardDuty 필터에 태그를 추가하려면 Amazon GuardDuty API 참조의 TagResource의 섹션을 참조하세요.

[GuardDuty.3] GuardDuty IPSets에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::GuardDuty::IPSet`

AWS Config규칙: `tagged-guardduty-ipset` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon GuardDuty IPSet에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. IPSet에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 IPSet에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

GuardDuty IPSet에 태그를 추가하려면 Amazon GuardDuty API 참조의 TagResource의 섹션을 참조하세요.

[GuardDuty.4] GuardDuty 탐지기에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config규칙: `tagged-guardduty-detector` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon GuardDuty 감지기에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 감지기에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 감지기에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

GuardDuty 탐지기에 태그를 추가하려면 Amazon GuardDuty API 참조의 TagResource의 섹션을 참조하세요.

[GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-eks-protection-audit-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 GuardDuty EKS 감사 로그 모니터링이 활성화되어 있는지 확인합니다. 독립형 계정의 경우, 계정에서 GuardDuty EKS 감사 로그 모니터링이 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정과 모든 멤버 계정에 EKS 감사 로그 모니터링이 활성화되어 있지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 다중 계정 환경에서는 GuardDuty 위임된 관리자 계정만 조직의 멤버 계정에 대해 EKS 감사 로그 모니터링 기능을 활성화 또는 비활성화할 수 있습니다. GuardDuty 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 GuardDuty 관리자에게 GuardDuty EKS 감사 로그 모니터링이 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 GuardDuty 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

EKS 감사 로그 모니터링을 사용하면 Amazon Elastic Kubernetes Service(Amazon EKS)의 EKS 클러스터에서 잠재적으로 의심스러운 활동을 탐지할 수 있습니다. EKS 감사 로그 모니터링은 Kubernetes 감사 로그를 사용하여 사용자, Kubernetes API를 사용하는 애플리케이션, 컨트롤 플레인의 시간순 활동을 캡처합니다.

문제 해결

GuardDuty EKS 감사 로그 모니터링을 활성화하려면 Amazon GuardDuty 사용 설명서의 EKS 감사 로그 모니터링을 참조하세요.

[GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/11.5.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-lambda-protection-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 GuardDuty Lambda 보호가 활성화되어 있는지 확인합니다. 독립형 계정의 경우, 계정에서 GuardDuty Lambda 보호가 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정과 모든 멤버 계정에 Lambda 보호가 활성화되지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 Lambda 보호 기능을 활성화하거나 비활성화할 수 있습니다. GuardDuty 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 GuardDuty 관리자에게 GuardDuty Lambda 보호가 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 GuardDuty 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

GuardDuty Lambda 보호는 AWS Lambda함수가 호출될 때 잠재적 보안 위협을 식별하는 데 도움이 됩니다. Lambda Protection을 활성화한 후 GuardDuty는 AWS 계정에 Lambda 함수와 연결된 Lambda 네트워크 활동 로그 모니터링을 시작합니다. Lambda 함수가 호출되고 GuardDuty가 Lambda 함수에서 잠재적 악성 코드가 있음을 나타내는 의심스러운 네트워크 트래픽을 식별하면 조사 결과를 생성합니다.

문제 해결

GuardDuty Lambda 보호를 활성화하려면 Amazon GuardDuty 사용 설명서의 Lambda 보호 구성을 참조하세요.

[GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/11.5.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-eks-protection-runtime-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 자동 에이전트 관리를 사용한 GuardDuty EKS 런타임 모니터링이 활성화되어 있는지 확인합니다. 독립 실행형 계정의 경우, 계정에서 자동 에이전트 관리를 사용한 GuardDuty EKS 런타임 모니터링이 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정과 모든 멤버 계정에 자동 에이전트 관리가 활성화된 EKS 런타임 모니터링이 없는 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대한 에이전트 자동 관리를 통해 EKS 런타임 모니터링 기능을 활성화하거나 비활성화할 수 있습니다. GuardDuty 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 GuardDuty 관리자에게 GuardDuty EKS 런타임 모니터링이 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 GuardDuty 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

Amazon GuardDuty의 EKS 보호는 AWS 환경 내에서 Amazon EKS 클러스터를 보호하는 데 도움이 되는 위협 적용 범위를 제공합니다. EKS 런타임 모니터링은 운영 체제 수준 이벤트를 사용하여 Amazon EKS 클러스터 내의 Amazon EKS 노드 및 컨테이너에서 잠재적 위협을 탐지하는 데 도움이 됩니다.

문제 해결

자동 에이전트 관리로 EKS 런타임 모니터링을 활성화하려면 Amazon GuardDuty 사용 설명서의 GuardDuty 런타임 모니터링 활성화를 참조하세요.

[GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-malware-protection-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 GuardDuty 맬웨어 보호가 활성화되어 있는지 확인합니다. 독립 실행형 계정의 경우, 계정에서 GuardDuty 멀웨어 보호가 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정과 모든 멤버 계정에 맬웨어 방지가 활성화되어 있지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 맬웨어 보호 기능을 활성화하거나 비활성화할 수 있습니다. GuardDuty 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 GuardDuty 관리자에게 GuardDuty 맬웨어 보호가 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 GuardDuty 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

EC2에 대한 GuardDuty 맬웨어 보호는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 컨테이너 워크로드에 연결된 Amazon Elastic Block Store(Amazon EBS) 볼륨을 스캔하여 맬웨어의 잠재적 존재를 탐지하는 데 도움이 됩니다. 맬웨어 보호는 스캔 시 특정 Amazon EC2 인스턴스 및 컨테이너 워크로드를 포함 또는 제외할지 결정할 수 있는 검사 옵션을 제공합니다. 또한 Amazon EC2 인스턴스 또는 컨테이너 워크로드에 연결된 Amazon EBS 볼륨의 스냅샷을 GuardDuty 계정에 보관하는 옵션도 제공합니다. 스냅샷은 맬웨어가 발견되고 맬웨어 보호 결과가 생성되는 경우에만 보관됩니다.

문제 해결

EC2에 대해 GuardDuty 맬웨어 보호를 활성화하려면 Amazon GuardDuty 사용 설명서의 GuardDuty 시작 맬웨어 스캔 구성 을 참조하세요.

[GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/11.5.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-rds-protection-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 GuardDuty RDS 보호가 활성화되어 있는지 확인합니다. 독립형 계정의 경우, 계정에서 GuardDuty RDS 보호가 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정과 모든 멤버 계정에 RDS 보호가 활성화되지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 RDS 보호 기능을 활성화하거나 비활성화할 수 있습니다. GuardDuty 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 GuardDuty 관리자에게

GuardDuty RDS 보호가 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, FAILED 조사 결과를 생성합니다. PASSED 조사 결과를 받으려면 위임된 관리자가 GuardDuty 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

Amazon GuardDuty의 RDS 보호 기능은 Amazon Aurora 데이터베이스(Amazon Aurora MySQL 호환 버전 및 Aurora PostgreSQL 호환 버전)에 대한 잠재적 액세스 위협에 대해 RDS 로그인 활동을 분석하고 프로파일링합니다. 이 기능을 사용하면 잠재적으로 의심스러운 로그인 동작을 식별할 수 있습니다. RDS 보호는 데이터베이스 인스턴스의 성능에 영향을 주지 않도록 설계되어 추가 인프라가 필요하지 않습니다. RDS 보호에서 데이터베이스에 대한 위협을 나타내는 잠재적으로 의심스럽거나 변칙적인 로그인 시도를 탐지하면 GuardDuty는 손상되었을지도 모르는 데이터베이스 관련 세부 정보가 포함된 새로운 탐지 결과를 생성합니다.

문제 해결

GuardDuty RDS Protection 활성화에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 GuardDuty RDS 보호를 참조하세요.

[GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/11.5.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: AWS::GuardDuty::Detector

AWS Config 규칙: guardduty-s3-protection-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 GuardDuty S3 보호가 활성화되어 있는지 확인합니다. 독립형 계정의 경우, 계정에서 GuardDuty S3 보호가 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정과 모든 멤버 계정에 S3 보호가 활성화되지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 S3 보호 기능을 활성화하거나 비활성화할 수 있습니다. GuardDuty 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 GuardDuty 관리자에게 GuardDuty S3 보호가 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, FAILED 조사 결과를 생성

합니다. PASSED 조사 결과를 받으려면 위임된 관리자가 GuardDuty 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

S3 보호는 GuardDuty가 객체 수준 API 작업을 모니터링하도록 활성화하여 Amazon Simple Storage Service(Amazon S3) 버킷 내 데이터에서 잠재적인 보안 위험을 식별하는 데 도움이 됩니다. GuardDuty는 AWS CloudTrail관리 이벤트와 CloudTrail S3 데이터 이벤트를 분석하여 S3 리소스에 대한 위협을 모니터링합니다.

문제 해결

GuardDuty S3 보호를 활성화하려면 Amazon GuardDuty 사용 설명서의 Amazon GuardDuty의 Amazon S3 보호를 참조하세요.

[GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-runtime-monitoring-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon GuardDuty에 런타임 모니터링이 활성화되어 있는지 확인합니다. 독립형 계정의 경우, 계정에서 GuardDuty 런타임 모니터링이 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정 및 모든 멤버 계정에 GuardDuty 런타임 모니터링이 활성화되어 있지 않은 경우 제어가 실패합니다.

다중 계정 환경에서는 위임된 GuardDuty 관리자만 조직의 계정에 대해 GuardDuty 런타임 모니터링을 활성화/비활성화할 수 있습니다. 또한 GuardDuty 관리자만 GuardDuty가 조직의 계정에 대해 AWS 워크로드 및 리소스의 런타임 모니터링에 사용하는 보안 에이전트를 구성하고 관리할 수 있습니다. GuardDuty 멤버 계정은 자신의 계정에 대해 런타임 모니터링을 활성화, 구성 또는 비활성화할 수 없습니다.

GuardDuty 런타임 모니터링은 운영 체제 수준, 네트워킹 및 파일 이벤트를 관찰하고 분석하여 환경의 특정 AWS워크로드에서 잠재적 위협을 탐지하는 데 도움이 됩니다. 런타임 모니터링은 파일 액세스, 프로세스 실행, 명령줄 인수 및 네트워크 연결과 같은 런타임 동작에 대한 가시성을 추가하는 GuardDuty 보안 에이전트를 사용합니다. Amazon EKS 클러스터, Amazon EC2 인스턴스 등 잠재적 위협을 모니터링하려는 각 리소스 유형에 대해 보안 에이전트를 활성화하고 관리할 수 있습니다.

문제 해결

GuardDuty 런타임 모니터링을 구성하고 활성화하는 방법에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 GuardDuty 런타임 모니터링 및 GuardDuty 런타임 모니터링 활성화를 참조하세요.

[GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다

범주: 감지 > 감지 서비스

심각도: 중간

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-ecs-protection-runtime-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS Fargate 기반 Amazon ECS 클러스터의 런타임 모니터링에 대해 Amazon GuardDuty 자동 보안 에이전트가 활성화되어 있는지 확인합니다. 독립형 계정의 경우 계정에서 보안 에이전트가 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정 및 모든 멤버 계정에 보안 에이전트가 활성화되지 않은 경우 제어가 실패합니다.

다중 계정 환경에서 이 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 이는 위임된 GuardDuty 관리자만 조직의 계정에 대한 ECS-Fargate 리소스의 런타임 모니터링을 활성화하거나 비활성화할 수 있기 때문입니다. GuardDuty 멤버 계정은 자신의 계정에 대해 이 작업을 수행할 수 없습니다. 또한 이 제어는 멤버 계정에서 GuardDuty가 일시 중지되고 ECS-Fargate 리소스의 런타임 모니터링이 비활성화된 경우 `FAILED` 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 GuardDuty 관리자가 GuardDuty를 사용하여 관리자 계정에서 일시 중지된 멤버 계정을 연결 해제해야 합니다.

GuardDuty 런타임 모니터링은 운영 체제 수준, 네트워킹 및 파일 이벤트를 관찰하고 분석하여 환경의 특정 AWS워크로드에서 잠재적 위협을 탐지하는 데 도움이 됩니다. 런타임 모니터링은 파일 액세스, 프로세스 실행, 명령줄 인수 및 네트워크 연결과 같은 런타임 동작에 대한 가시성을 추가하는 GuardDuty 보안 에이전트를 사용합니다. 잠재적 위협을 모니터링하려는 각 리소스 유형에 대해 보안 에이전트를 활성화하고 관리할 수 있습니다. 여기에는 AWS Fargate 기반 Amazon ECS 클러스터가 포함됩니다.

문제 해결

ECS-Fargate 리소스의 GuardDuty 런타임 모니터링에 대해 보안 에이전트를 활성화하고 관리하려면 GuardDuty를 직접 사용해야 합니다. ECS-Fargate 리소스에는 수동으로 활성화하거나 관리할 수 없

습니다. 보안 에이전트 활성화 및 관리에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 AWS Fargate(Amazon ECS만 해당) 지원을 위한 사전 조건 및 AWS Fargate(Amazon ECS만 해당)에 대한 자동 보안 에이전트 관리를 참조하세요.

[GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다

범주: 감지 > 감지 서비스

심각도: 중간

리소스 유형: `AWS::GuardDuty::Detector`

AWS Config 규칙: guardduty-ec2-protection-runtime-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon EC2 인스턴스의 런타임 모니터링에 대해 Amazon GuardDuty 자동 보안 에이전트가 활성화되어 있는지 확인합니다. 독립형 계정의 경우 계정에서 보안 에이전트가 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 GuardDuty 관리자 계정 및 모든 멤버 계정에 보안 에이전트가 활성화되지 않은 경우 제어가 실패합니다.

다중 계정 환경에서 이 제어는 위임된 GuardDuty 관리자 계정에서만 조사 결과를 생성합니다. 이는 위임된 GuardDuty 관리자만 조직의 계정에 대한 Amazon EC2 인스턴스의 런타임 모니터링을 활성화하거나 비활성화할 수 있기 때문입니다. GuardDuty 멤버 계정은 자신의 계정에 대해 이 작업을 수행할 수 없습니다. 또한 이 제어는 멤버 계정에서 GuardDuty가 일시 중지되고 EC2 인스턴스의 런타임 모니터링이 비활성화된 경우 `FAILED` 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 GuardDuty 관리자가 GuardDuty를 사용하여 관리자 계정에서 일시 중지된 멤버 계정을 연결 해제해야 합니다.

GuardDuty 런타임 모니터링은 운영 체제 수준, 네트워킹 및 파일 이벤트를 관찰하고 분석하여 환경의 특정 AWS워크로드에서 잠재적 위협을 탐지하는 데 도움이 됩니다. 런타임 모니터링은 파일 액세스, 프로세스 실행, 명령줄 인수 및 네트워크 연결과 같은 런타임 동작에 대한 가시성을 추가하는 GuardDuty 보안 에이전트를 사용합니다. 잠재적 위협을 모니터링하려는 각 리소스 유형에 대해 보안 에이전트를 활성화하고 관리할 수 있습니다. 여기에는 Amazon EC2 인스턴스가 포함됩니다.

문제 해결

EC2 인스턴스의 GuardDuty 런타임 모니터링에 대해 자동 보안 에이전트를 구성하고 관리하는 방법에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 Amazon EC2 인스턴스 지원을 위한 사전 조건 및 Amazon EC2 인스턴스에 대한 자동 보안 에이전트 활성화를 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Identity and Access Management

이러한 AWS Security Hub CSPM제어는 AWS Identity and Access Management(IAM) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v1.2.0/1.22, CIS AWS파운데이션 벤치마크 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, NIST.800-53.r5 AC-6(10), NISTNIST.800-53.r5 AC-6 AC

범주: 보호 > 보안 액세스 관리

심각도: 높음

리소스 유형: `AWS::IAM::Policy`

AWS Config 규칙: `iam-policy-no-statements-with-admin-access`

스케줄 유형: 변경이 트리거됨

파라미터:

- `excludePermissionBoundaryPolicy: true`(사용자 지정할 수 없음)

이 제어는 `"Resource": "*"`에 대해 `"Effect": "Allow"`과 `"Action": "*"`이 있는 문을 포함하여 기본 버전의 IAM 정책(고객 관리형 정책이라고도 함)에 관리자 액세스 권한이 있는지 확인합니다. 이러한 문이 포함된 IAM 정책이 있으면 제어가 실패합니다.

제어는 사용자가 생성한 고객 관리형 정책만 확인합니다. 인라인 및 AWS관리형 정책은 확인하지 않습니다.

IAM 정책에서는 사용자, 그룹 또는 역할에 부여되는 권한 세트를 정의합니다. 표준 보안 권고에 따라는 최소 권한을 부여할 것을 AWS권장합니다. 즉, 작업을 수행하는 데 필요한 권한만 부여해야 합니다. 사용자에게 있어야 하는 최소한의 권한 집합으로 제한하지 않고 전체 관리 권한을 제공하면 리소스가 원치 않는 작업에 노출될 수 있습니다.

전체 관리 권한을 허용하는 대신 사용자가 해야 할 작업을 파악한 후 해당 작업만 수행하도록 정책을 작성합니다. 최소한의 권한 집합으로 시작하여 필요에 따라 추가 권한을 부여하는 것이 안전합니다. 처음부터 권한을 많이 부여하지 말고 나중에 강화하세요.

`"Resource": "*"`에 대해 `"Effect": "Allow"` 과 `"Action": "*"`이 있는 문이 있는 IAM 정책을 제거해야 합니다.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

전체 '*' 관리 권한이 허용되지 않도록 IAM 정책을 수정하려면 IAM 사용자 설명서의 IAM 정책 편집을 참조하세요.

[IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.14, CIS AWS파운데이션 벤치마크 v3.0.0/1.15, CIS AWS파운데이션 벤치마크 v1.2.0/1.16, 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-6, NIST.800-53.r5 AC-6(3), NIST.800-171.r1.r1.r

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `iam-user-no-policies-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 IAM 사용자에게 정책이 연결되어 있는지 확인합니다. IAM 사용자에게 정책이 연결되어 있는 경우, 제어가 실패합니다. 대신 IAM 사용자는 IAM 그룹에서 권한을 상속하거나 역할을 맡아야 합니다.

기본적으로 IAM 사용자, 그룹 및 역할은 AWS리소스에 액세스할 수 없습니다. IAM 정책은 사용자, 그룹 또는 역할에 권한을 부여하는 방법입니다. IAM 정책을 사용자가 아닌 그룹 및 역할에 직접 적용하는 것이 좋습니다. 그룹 또는 역할 수준에서 권한을 지정하면 사용자 수가 증가할 때 액세스 관리 복잡성

이 줄어듭니다. 액세스 관리 복잡성을 줄이면 보안 주체가 부주의로 과도한 권한을 받거나 보유할 기회가 줄어듭니다.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

이 문제를 해결하려면 IAM 그룹을 생성하고 정책을 그룹에 연결하세요. 그런 다음 사용자를 그룹에 추가합니다. 정책은 그룹 내 각 사용자에게 적용됩니다. 사용자에게 직접 연결된 정책을 제거하려면 IAM 사용자 설명서의 IAM ID 권한 추가 및 제거를 참조하세요.

[IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.13, CIS AWS파운데이션 벤치마크 v3.0.0/1.14, CIS AWS파운데이션 벤치마크 v1.4.0/1.14, CIS AWS파운데이션 벤치마크 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `access-keys-rotated`

스케줄 유형: 주기적

파라미터:

- `maxAccessKeyAge`: `90`(사용자 지정할 수 없음)

이 제어는 활성 액세스 키가 90일마다 교체되는지 여부를 확인합니다.

사용자 계정에서 모든 액세스 키를 생성 및 제거하지 않는 것이 좋습니다. 대신 권장되는 모범 사례는 하나 이상의 IAM 역할을 생성하거나 페더레이션을 사용하는 것입니다AWS IAM Identity Center. 이러

한 방법을 사용하여 사용자가 AWS Management Console및에 액세스하도록 허용할 수 있습니다AWS CLI.

각 접근법에는 사용 사례가 있습니다. 페더레이션은 일반적으로 기존 중앙 디렉터리가 있거나 IAM 사용자에 대한 현재 제한보다 더 많은 것이 필요할 것으로 예상되는 기업에 더 좋습니다. AWS환경 외부에서 실행되는 애플리케이션은 AWS리소스에 프로그래밍 방식으로 액세스하려면 액세스 키가 필요합니다.

그러나 프로그래밍 방식 액세스가 필요한 리소스가 내부에서 실행되는 경우 IAM 역할을 사용하는 것이 AWS가장 좋습니다. 역할을 사용하면 액세스 키 ID 및 보안 액세스 키를 구성에 하드 코딩하지 않고도 리소스 액세스 권한을 부여할 수 있습니다.

액세스 키 및 계정 보호에 대한 자세한 내용은의 AWS액세스 키 관리 모범 사례를 참조하세요AWS 일반 참조. 또한 프로그래밍 방식 액세스를 사용하는 AWS 계정동안를 보호하기 위한 지침 블로그 게시물을 참조하세요.

액세스 키가 이미 있는 경우 Security Hub CSPM은 90일마다 액세스 키를 교체할 것을 권장합니다. 액세스 키를 교체하면 손상되거나 종료된 계정에 연결된 액세스 키가 사용될 가능성이 줄어듭니다. 또한 분실, 해킹 또는 도용된 기존 키로 데이터에 액세스할 수 없도록 합니다. 액세스 키를 교체한 후에는 항상 애플리케이션을 업데이트하세요.

액세스 키는 액세스 키 ID와 보안 액세스 키로 구성되어 있습니다. 이 키들은 AWS에 보내는 프로그래밍 방식의 요청에 서명하는 데 사용됩니다. 사용자는 , Tools for Windows PowerShellAWS CLI, AWSSDKsAWS에서를 프로그래밍 방식으로 호출하거나 개별 API 작업을 사용하여 HTTP 직접 호출을 수행하려면 자체 액세스 키가 필요합니다AWS 서비스.

조직에서 AWS IAM Identity Center(IAM Identity Center)를 사용하는 경우 사용자는 Active Directory, 내장 IAM Identity Center 디렉터리 또는 IAM Identity Center에 연결된 다른 ID 제공업체(IdP)에 로그인할 수 있습니다. 그런 다음 액세스 키 없이 AWS CLI명령을 실행하거나 AWSAPI 작업을 호출할 수 있는 IAM 역할에 매핑할 수 있습니다. 자세한 내용은 AWS Command Line Interface사용 설명서의 AWS CLI를 사용하도록 구성을 AWS IAM Identity Center 참조하세요.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

90일이 지난 액세스 키를 교체하려면 IAM 사용자 설명서의 액세스 키 교체를 참조하세요. 액세스 키 사용 기간이 90일 이상인 모든 사용자의 지침을 따르세요.

[IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.3, CIS AWS파운데이션 벤치마크 v3.0.0/1.4, CIS AWS파운데이션 벤치마크 v1.4.0/1.4, CIS AWS파운데이션 벤치마크 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

범주: 보호 > 보안 액세스 관리

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-root-access-key-check`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 루트 사용자 액세스 키가 존재하는지 확인합니다.

루트 사용자는 aAWS 계정.AWSaccess 키에서 가장 권한이 있는 사용자이며 지정된 계정에 프로그래밍 방식으로 액세스할 수 있습니다.

Security Hub CSPM은 루트 사용자와 연결된 모든 액세스 키를 제거할 것을 권장합니다. 이렇게 하면 계정을 손상시킬 수 있는 벡터가 제한됩니다. 권한이 가장 적은 역할 기반 계정을 만들고 사용할 수도 있습니다.

문제 해결

루트 사용자 액세스 키를 삭제하려면 IAM 사용자 설명서의 루트 사용자의 액세스 키 삭제를 참조하세요. 의 AWS 계정에서 루트 사용자 액세스 키를 삭제하려면 AWS GovCloud (US)사용 설명서의 내 AWS GovCloud (US)계정 루트 사용자 액세스 키 삭제를 AWS GovCloud (US)참조하세요.

[IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.9, CIS AWS파운데이션 벤치마크 v3.0.0/1.10, CIS AWS파운데이션 벤치마크 v1.4.0/1.10, CIS AWS파운데이션 벤치마크 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), NIST.800-53.r5 IA-2(6), NIST.800-53.r5 IA-53.r5 IA-2(6), N

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `mfa-enabled-for-iam-console-access`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 콘솔 암호를 사용하는 모든 IAM 사용자에 대해 AWS다중 인증(MFA)이 활성화되어 있는지 확인합니다.

다중 인증(MFA)을 통해 사용자 이름 및 비밀번호 외에 보호 계층이 한 단계 더 추가됩니다. MFA를 활성화하면 사용자가 AWS웹 사이트에 로그인하면 사용자 이름과 암호를 입력하라는 메시지가 표시됩니다. 또한 AWSMFA 디바이스에서 인증 코드를 입력하라는 메시지가 표시됩니다.

콘솔 암호가 있는 모든 계정에 대해 MFA를 활성화하는 것이 좋습니다. MFA는 콘솔 액세스의 보안을 강화하도록 설계되었습니다. 인증 보안 주체는 시간에 민감한 키를 내보내는 디바이스를 가지고 있어야 하며 보안 인증에 대한 지식이 있어야 합니다.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

IAM 사용자를 위한 MFA를 추가하려면 IAM 사용자 설명서의 AWS에서의 다중 인증(MFA) 사용을 참조하세요.

[IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.5, CIS AWS파운데이션 벤치마크 v3.0.0/1.6, CIS AWS파운데이션 벤치마크 v1.4.0/1.6, CIS AWS파운데이션 벤치마크 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), NIST.800-53.r5 IA-2

범주: 보호 > 보안 액세스 관리

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `root-account-hardware-mfa-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어AWS 계정는가 하드웨어 다중 인증(MFA) 디바이스를 사용하여 루트 사용자 자격 증명으로 로그인하도록 활성화되어 있는지 확인합니다. 하드웨어 MFA가 활성화되지 않았거나 가상 MFA 디바이스가 루트 사용자 자격 증명으로 로그인하도록 허용된 경우 제어가 실패합니다.

가상 MFA는 하드웨어 MFA 디바이스와 동일한 수준의 보안을 제공하지 않을 수 있습니다. 하드웨어 구매 승인 또는 하드웨어 도착을 기다리는 동안 가상 MFA 디바이스만 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용자 설명서의 가상 MFA 디바이스 할당(콘솔)을 참조하세요.

> **Note**
>
> Security Hub CSPM은에 루트 사용자 자격 증명(로그인 프로필)이 있는지 여부를 기반으로이 제어를 평가합니다AWS 계정. 제어는 다음과 같은 경우, `PASSED` 조사 결과를 생성합니다.
>
> - 계정에 루트 사용자 자격 증명이 있고 루트 사용자에 대해 하드웨어 MFA가 활성화되어 있습니다.
> - 계정에 루트 사용자 자격 증명이 없습니다.
>
> 계정에 루트 사용자 자격 증명이 있고 루트 사용자에 대해 하드웨어 MFA가 활성화되지 않은 경우 제어가 `FAILED` 조사 결과를 생성합니다.

문제 해결

루트 사용자에 대해 하드웨어 MFA를 활성화하는 방법에 대한 자세한 내용은 IAM 사용자 설명서의 AWS 계정 루트 사용자에 대한 다중 인증을 참조하세요.

[IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

관련 요구 사항: 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 IA-5(1), NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `RequireUppercaseCharacters` | 암호에 대문자가 한 개 이상 있어야 합니다. | 부울 | `true` 또는 `false` | `true` |
| `RequireLowercaseCharacters` | 암호에 소문자가 한 개 이상 있어야 합니다. | 부울 | `true` 또는 `false` | `true` |
| `RequireSymbols` | 암호에 기호가 한 개 이상 있어야 합니다. | 부울 | `true` 또는 `false` | `true` |
| `RequireNumbers` | 암호에 숫자가 한 개 이상 있어야 합니다. | 부울 | `true` 또는 `false` | `true` |
| `MinimumPasswordLength` | 암호의 최소 특수 문자 수 | Integer | 8~128 | 8 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| PasswordReusePrevention | 이전 암호를 다시 사용할 수 있을 때까지의 암호 순환 횟수 | Integer | 12~24 | 기본값 없음 |
| MaxPasswordAge | 암호 만료까지 남은 일수 | Integer | 1~90 | 기본값 없음 |

이 제어는 IAM 사용자에 대한 계정 암호 정책이 강력한 구성을 사용하는지 확인합니다. 암호 정책에서 강력한 구성을 사용하지 않으면 제어가 실패합니다. 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 이전 표에 언급된 기본값을 사용합니다. PasswordReusePrevention 및 MaxPasswordAge 파라미터에는 기본값이 없으므로 이러한 파라미터를 제외하면 Security Hub CSPM은이 제어를 평가할 때 암호 교체 횟수와 암호 수명을 무시합니다.

에 액세스하려면 AWS Management ConsoleIAM 사용자에게 암호가 필요합니다. Security Hub CSPM은 IAM 사용자를 생성하는 대신 페더레이션을 사용할 것을 적극 권장합니다. 페더레이션을 통해 사용자는 기존 기업 보안 인증을 사용하여 AWS Management Console에 로그인할 수 있습니다. AWS IAM Identity Center(IAM Identity Center)를 사용하여 사용자를 생성하거나 페더레이션한 다음 IAM 역할을 계정으로 수임합니다.

ID 공급자 및 페더레이션에 대해 자세히 알아보려면 IAM 사용자 설명서의 ID 제공업체 및 페더레이션을 참조하세요. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서를 참조하세요.

IAM 사용자를 사용해야 하는 경우 Security Hub CSPM은 강력한 사용자 암호 생성을 적용할 것을 권장합니다. 에서 암호 정책을 설정AWS 계정하여 암호의 복잡성 요구 사항과 필수 교체 기간을 지정할 수 있습니다. 비밀번호 정책을 생성 또는 변경하더라도 대부분의 비밀번호 정책 설정은 사용자가 다음에 자신의 비밀번호를 변경할 때 적용됩니다. 일부 설정은 바로 적용됩니다.

문제 해결

암호 정책을 업데이트하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 암호 정책 설정을 참조하세요.

[IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 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(7), NIST.800-53.r5 AC-6, NIST.800-171.r2 3.1.2, PCI DSS v3.2.1/8.1.4, PCI DSS v4.0.1/8.2.6 NIST.800-53.r5 AC-3

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `iam-user-unused-credentials-check`

스케줄 유형: 주기적

파라미터:

- `maxCredentialUsageAge`: `90`(사용자 지정할 수 없음)

이 제어는 IAM 사용자에게 90일 동안 사용되지 않은 암호 또는 활성 액세스 키가 있는지 확인합니다.

IAM 사용자는 암호 또는 액세스 키와 같은 다양한 유형의 자격 증명을 사용하여 AWS리소스에 액세스할 수 있습니다.

Security Hub CSPM은 90일 이상 사용하지 않은 모든 자격 증명을 제거하거나 비활성화할 것을 권장합니다. 불필요한 보안 인증을 비활성화하거나 제거하면 침해되거나 버려진 계정과 연결된 보안 인증이 사용될 가능성이 줄어듭니다.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

IAM 콘솔에서 사용자 정보를 보면 액세스 키 사용 기간, 비밀번호 사용 기간, 마지막 활동 열이 표시됩니다. 이 열 중 어느 하나라도 값이 90일보다 큰 경우, 해당 사용자의 보안 인증을 비활성화하세요.

또한 보안 인증 보고서를 사용해 사용자를 모니터링하고 90일 이상 활동이 없는 사용자를 식별할 수 있습니다. IAM 콘솔에서 `.csv` 형식으로 된 보안 인증 정보 보고서를 다운로드할 수 있습니다.

비활성 계정이나 사용하지 않는 보안 인증 정보를 식별한 후에는 비활성화하세요. 자세한 지침은 IAM 사용자 설명서의 IAM 사용자 암호 생성, 변경 또는 삭제(콘솔)를 참조하세요.

[IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.4, PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2, CIS AWS파운데이션 벤치마크 v3.0.0/1.5, CIS AWS파운데이션 벤치마크 v1.4.0/1.5, CIS AWS파운데이션 벤치마크 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(2), NIST.800-53.r5 IA-2

범주: 보호 > 보안 액세스 관리

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: `root-account-mfa-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는의 IAM 루트 사용자가에 로그인할 수 AWS 계정있도록 다중 인증(MFA)이 활성화되어 있는지 확인합니다AWS Management Console. 계정의 루트 사용자에 대해 MFA가 활성화되어 있지 않으면 제어가 실패합니다.

의 IAM 루트 사용자는 계정의 모든 서비스 및 리소스에 대한 완전한 액세스 권한을 AWS 계정가집니다. MFA가 활성화된 경우 사용자는에 로그인하기 위해 AWSMFA 디바이스의 사용자 이름, 암호 및 인증 코드를 입력해야 합니다AWS Management Console. MFA를 통해 사용자 이름 및 암호 외에 보호 계층이 한 단계 더 추가됩니다.

이 제어는 다음과 같은 경우 `PASSED` 조사 결과를 생성합니다.

- 계정에 루트 사용자 자격 증명이 있고 루트 사용자에 대해 MFA가 활성화되어 있습니다.
- 계정에 루트 사용자 자격 증명이 없습니다.

계정에 루트 사용자 자격 증명이 있고 루트 사용자에 대해 MFA가 활성화되지 않은 경우 제어가 `FAILED` 조사 결과를 생성합니다.

문제 해결

의 루트 사용자에 대해 MFA를 활성화하는 방법에 대한 자세한 내용은 AWS Identity and Access Management사용 설명서의 에 대한 멀티 팩터 인증을AWS 계정 루트 사용자 AWS 계정참조하세요.

[IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.

관련 요구 사항: NIST.800-171.r2 3.5.2, NIST.800-171.r2 3.5.7, NIST.800-171.r2 3.5.8, PCI DSS 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 IAM 사용자에 대한 계정 비밀번호 정책이 다음 최소 PCI DSS 구성을 사용하는지 확인합니다.

- `RequireUppercaseCharacters` – 암호에 대문자가 한 개 이상이어야 합니다. (기본값은 `true`)
- `RequireLowercaseCharacters` – 암호에 소문자가 한 개 이상이어야 합니다. (기본값은 `true`)
- `RequireNumbers` – 암호에 숫자가 한 개 이상이어야 합니다. (기본값은 `true`)
- `MinimumPasswordLength` – 암호 최소 길이입니다. (기본값은 7 이상)
- `PasswordReusePrevention` – 재사용을 허가받기까지 사용할 수 있는 암호 개수입니다. (기본값은 4)
- `MaxPasswordAge` - 암호 만료까지 남은 일수입니다. (기본값은 90)

> **Note**
>
> 2025년 5월 30일에 Security Hub CSPM은 PCI DSS v4.0.1 표준에서이 제어를 제거했습니다. PCI DSS v4.0.1은 이제 최소 암호 길이로 8자를 요구합니다. 암호 요구 사항이 다른 PCI DSS v3.2.1 표준에는 이 제어가 계속 적용됩니다.
> PCI DSS v4.0.1 요구 사항을 기준으로 계정 암호 정책을 평가하려면 IAM.7 제어를 사용할 수 있습니다. 이 제어는 최소 암호 길이로 8자를 요구합니다. 또한 암호 길이 및 기타 파라미터에

대한 사용자 지정 값도 지원합니다. IAM.7 제어는 Security Hub CSPM의 PCI DSS v4.0.1 표준의 일부입니다.

문제 해결

권장 구성을 사용하도록 암호 정책을 업데이트하려면 IAM 사용자 설명서의 IAM 사용자에 대한 계정 비밀번호 정책 설정을 참조하세요.

[IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다.

CIS는 비밀번호 정책에 하나 이상의 대문자를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

문제 해결

비밀번호 정책을 변경하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하세요. 비밀번호 강도에서 라틴 알파벳(A~Z) 중 하나 이상의 대문자 요구를 선택합니다.

[IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다. CIS에서는 비밀번호 정책에 하나 이상의 소문자를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

문제 해결

비밀번호 정책을 변경하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하세요. 비밀번호 강도에서 라틴 알파벳(A~Z) 중 하나 이상의 소문자 요구를 선택합니다.

[IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS AWSFoundations Benchmark v1.2.0/1.7, NIST.800-171.r2 3.5.7

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다.

CIS에서는 비밀번호 정책에 하나 이상의 기호를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

문제 해결

비밀번호 정책을 변경하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하세요. 비밀번호 강도에서 하나 이상의 영숫자가 아닌 문자 요구를 선택합니다.

[IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호에 다양한 문자 집합이 사용되도록 합니다.

CIS에서는 비밀번호 정책에 하나 이상의 숫자를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

문제 해결

비밀번호 정책을 변경하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하세요. 비밀번호 강도에서 하나 이상의 숫자 요구를 선택합니다.

[IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.7, CIS AWS파운데이션 벤치마크 v3.0.0/1.8, CIS AWS파운데이션 벤치마크 v1.4.0/1.8, CIS AWS파운데이션 벤치마크 v1.2.0/1.9, NIST.800-171.r2 3.5.7

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

암호 정책은 부분적으로 암호 복잡성 요건을 강제합니다. IAM 비밀번호 정책을 사용하여 비밀번호가 지정된 길이 이상이 되도록 합니다.

CIS에서는 비밀번호 정책에 최소 14자의 비밀번호 길이를 요구할 것을 권장합니다. 비밀번호 복잡성 정책을 설정하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

문제 해결

비밀번호 정책을 변경하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하세요. 비밀번호의 최소 길이에 **14** 또는 더 큰 숫자를 입력합니다.

[IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.8, CIS AWS파운데이션 벤치마크 v3.0.0/1.9, CIS AWS파운데이션 벤치마크 v1.4.0/1.9, CIS AWS파운데이션 벤치마크 v1.2.0/1.10, NIST.800-171.r2 3.5.8, PCI DSS v4.0.1/8.3.7

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 기억할 암호 수가 24개로 설정되어 있는지 확인합니다. 값이 24가 아니면 제어가 실패합니다.

IAM 비밀번호 정책은 동일한 사용자가 특정 비밀번호를 재사용하는 것을 방지할 수 있습니다.

CIS에서는 비밀번호 정책을 통해 비밀번호 재사용을 방지할 것을 권장합니다. 암호 재사용을 방지하면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다.

문제 해결

비밀번호 정책을 변경하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하세요. 비밀번호 재사용 방지에 **24**를 입력합니다.

[IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v1.2.0/1.11, PCI DSS v4.0.1/8.3.9, PCI DSS v4.0.1/8.3.10.1

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-password-policy`

스케줄 유형: 주기적

파라미터: 없음

IAM 암호 정책에서는 지정된 일수 후에 암호를 교체하거나 만료하도록 요구할 수 있습니다.

CIS는 비밀번호 정책에서 비밀번호가 90일 이내에 만료되도록 권장합니다. 비밀번호 수명을 줄이면 무차별 로그인 시도에 대한 계정 복원력이 향상됩니다. 또한 정기적으로 비밀번호를 변경하도록 하면 다음과 같은 시나리오에 도움이 됩니다.

- 비밀번호는 지식이 없어도 도용하거나 침해할 수 있습니다. 이러한 일은 시스템 침해, 소프트웨어 취약점 또는 인터넷 위협을 통해 발생합니다.
- 암호화된 트래픽이라도 특정 기업 및 정부 웹 필터 또는 프록시 서버가 가로채 기록할 수 있습니다.
- 많은 사람들은 업무, 이메일, 개인 용도로 여러 시스템에 동일한 비밀번호를 사용합니다.
- 침해된 최종 사용자 워크스테이션에는 키 입력 로거가 있을 수 있습니다.

문제 해결

비밀번호 정책을 변경하려면 IAM 사용자 설명서의 IAM 사용자를 위한 계정 비밀번호 정책 설정을 참조하세요. 비밀번호 만료 활성화에 **90** 또는 더 작은 숫자를 입력하세요.

[IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.16, CIS AWS파운데이션 벤치마크 v3.0.0/1.17, CIS AWS파운데이션 벤치마크 v1.4.0/1.17, CIS AWS파운데이션 벤치마크 v1.2.0/1.20, NIST.800-171.r2 3.1.2, PCI DSS v4.0.1/12.10.3

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `iam-policy-in-use`

스케줄 유형: 주기적

파라미터:

- `policyARN`: `arn:partition:iam::aws:policy/AWSSupportAccess`(사용자 지정할 수 없음)
- `policyUsageType`: `ANY`(사용자 지정할 수 없음)

AWS는 인시던트 알림 및 대응, 기술 지원 및 고객 서비스에 사용할 수 있는 지원 센터를 제공합니다.

AWS 지원을 통해 권한 있는 사용자가 인시던트를 관리할 수 있도록 IAM 역할을 생성합니다. IAM 역할에는 액세스 제어에 대한 최소 권한을 구현하여 인시던트를 관리하기 위해 지원 센터 액세스를 허용하는 적절한 IAM 정책이 필요합니다지원.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

이 문제를 해결하려면 권한이 있는 사용자가 지원 인시던트를 관리할 수 있도록 허용하는 역할을 생성합니다.

지원액세스에 사용할 역할을 생성하려면

1. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
2. IAM 탐색 창에서 역할을 선택한 후 역할 생성을 선택합니다.
3. 역할 유형에서 다른 AWS 계정을 선택합니다.
4. 계정 ID에 리소스AWS 계정에 대한 액세스 권한을 부여하려는의 AWS 계정ID를 입력합니다.

   이 역할을 수임할 사용자 또는 그룹이 동일한 계정에 있는 경우, 로컬 계정 번호를 입력합니다.

   > **Note**
   >
   > 지정된 계정의 관리자는 해당 계정의 모든 사용자에게 이 역할을 맡을 수 있는 권한을 부여할 수 있습니다. 이를 위해 관리자는 `sts:AssumeRole` 작업에 대한 권한을 부여하는 정책을 사용자나 그룹에 연결합니다. 이 정책에서 리소스는 역할 ARN이어야 합니다.

5. 다음: 권한을 선택합니다.
6. 관리형 정책 `AWSSupportAccess`를 검색합니다.
7. `AWSSupportAccess` 관리형 정책의 확인란을 선택합니다.
8. 다음: 태그를 선택합니다.
9. (선택 사항) 역할에 메타데이터를 추가하려면 태그를 키-값 쌍으로 연결합니다.

   IAM에서 태그 사용에 대한 자세한 내용을 알아보려면 IAM 사용자 설명서의 IAM 사용자 및 역할 태그 지정을 참조하세요.
10. 다음: 검토를 선택합니다.
11. 역할 이름에 역할의 이름을 입력합니다.

    역할 이름은 내에서 고유해야 합니다AWS 계정. 이메일은 대소문자를 구분하지 않습니다.
12. (선택 사항)역할 설명에 새로운 역할에 대한 설명을 입력합니다.
13. 역할을 검토한 후 역할 생성을 선택합니다.

[IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

관련 요구 사항: 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), NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.5.3, NIST.800-171.r2 3.5.4, NIST.800-171.r2 3.7.5, PCI DSS v3.2.1/8.3.1, PCI DSS v4.0.1/8.4.2,

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config 규칙: `iam-user-mfa-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 IAM 사용자가 다중 인증(MFA)을 활성화했는지 여부를 확인합니다.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

IAM 사용자를 위한 MFA를 추가하려면 IAM 사용자 설명서의 AWS 사용자를 위한 MFA 디바이스 활성화를 참조하세요.

[IAM.20] 루트 사용자의 사용을 피합니다.

> **Important**
>
> Security Hub CSPM은 2024년 4월에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그 단원을 참조하십시오.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v1.2.0/1.1

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::IAM::User`

AWS Config규칙: `use-of-root-account-test` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 주기적

파라미터: 없음

이 제어AWS 계정는에 루트 사용자의 사용에 대한 제한이 있는지 확인합니다. 이 제어는 다음 리소스를 평가합니다.

- Amazon Simple Notification Service(SNS) 주제
- AWS CloudTrail추적
- CloudTrail 추적과 연결된 메트릭 필터
- 필터 기반 Amazon CloudWatch 경보

다음 문 중 하나 이상이 참인 경우, 이 검사는 `FAILED` 조사 결과가 됩니다.

- 계정에 CloudTrail 트레일이 없습니다.
- CloudTrail 추적이 활성화되었지만 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 구성되지 않았습니다.
- CloudTrail 추적이 활성화되었지만 CloudWatch Logs 로그 그룹과 연결되지 않았습니다.
- CIS(인터넷 보안 센터)에서 규정한 정확한 메트릭 필터는 사용되지 않습니다. 규정된 메트릭 필터는 `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType !="AwsServiceEvent"}'`입니다.
- 메트릭 필터를 기반으로 하는 CloudWatch 경보가 계정에 존재하지 않습니다.
- 관련 SNS 주제에 알림을 보내도록 구성된 CloudWatch 경보는 경보 조건에 따라 트리거되지 않습니다.
- SNS 주제는 SNS 주제에 메시지를 전송하기 위한 제약 조건을 준수하지 않습니다.
- SNS 주제에 구독자가 한 명 이상 없습니다.

다음 문 중 하나 이상이 참인 경우, 이 검사를 통해 제어 상태는 `NO_DATA`이 됩니다.

- 다중 리전 추적은 다른 리전을 기반으로 합니다. Security Hub CSPM은 추적의 기반이 되는 리전에서만 조사 결과를 생성할 수 있습니다.
- 다중 리전 추적은 다른 계정에 속합니다. Security Hub CSPM은 추적을 소유한 계정에 대해서만 조사 결과를 생성할 수 있습니다.

다음 문 중 하나 이상이 참인 경우, 이 검사를 통해 제어 상태는 WARNING이 됩니다.

- 현재 계정은 CloudWatch 경보에서 참조되는 SNS 주제를 소유하지 않습니다.
- 현재 계정은 ListSubscriptionsByTopic SNS API 호출 시 해당 SNS 주제에 접근할 수 없습니다.

> **Note**
>
> 조직 추적을 사용하여 조직 내 여러 계정의 이벤트를 기록하는 것이 좋습니다. 조직 추적은 기본적으로 다중 리전 추적이며 AWS Organizations관리 계정 또는 CloudTrail 위임된 관리자 계정에서만 관리할 수 있습니다. 조직 추적을 사용하면 조직 구성원 계정에서 평가된 제어에 대한 제어 상태가 NO_DATA가 됩니다. 멤버 계정에서 Security Hub CSPM은 멤버 소유 리소스에 대한 조사 결과만 생성합니다. 조직 추적과 관련된 조사 결과는 리소스 소유자 계정에서 생성됩니다. 교차 리전 집계를 사용하여 Security Hub CSPM 위임된 관리자 계정에서 이러한 결과를 볼 수 있습니다.

계정 및 서비스 관리 작업 수행에 필요한 경우에만 루트 사용자 보안 인증 정보를 사용하는 것이 가장 좋습니다. IAM 정책을 사용자가 아닌 그룹 및 역할에 직접 적용하세요. 일상적인 사용을 위해 관리자를 설정하는 방법에 대한 지침은 IAM 사용자 설명서의 첫 번째 IAM 관리자 및 그룹 생성을 참조하세요.

문제 해결

이 문제를 해결하는 단계에는 Amazon SNS 주제, CloudTrail 추적, 메트릭 필터 및 메트릭 필터에 대한 경보 설정이 포함됩니다.

Amazon SNS 토픽을 생성하려면

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 모든 CIS 경보를 수신하는 Amazon SNS 주제를 생성합니다.

   이 주제에 대해 하나 이상의 구독자를 생성합니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 시작하기를 참조하세요.

다음으로 모든 리전에 적용되는 활성 CloudTrail을 설정합니다. 이렇게 하려면 the section called "[CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다."의 문제 해결 절차를 따르세요.

CloudTrail 추적과 연결하는 CloudWatch Logs 로그 그룹의 이름을 기록해 둡니다. 로그 그룹에 대한 메트릭 필터를 생성합니다.

마지막으로 메트릭 필터와 경보를 생성합니다.

메트릭 필터 및 경보를 생성하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 로그 그룹을 선택합니다.
3. 생성한 CloudTrail 추적과 연결된 CloudWatch Logs 로그 그룹의 확인란을 선택합니다.
4. 작업에서 메트릭 필터 생성을 선택합니다.
5. 패턴 정의에 대해 다음을 수행합니다.

   a. 다음 패턴을 복사하여 필터 패턴 필드에 붙여 넣습니다.

   ```
   {$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS &&
    $.eventType !="AwsServiceEvent"}
   ```

   b. 다음을 선택합니다.
6. 메트릭 할당에서 다음 작업을 수행합니다.

   a. 필터 이름에 메트릭 필터의 이름을 입력합니다.

   b. 메트릭 네임스페이스에 **`LogMetrics`**를 입력합니다.

      모든 CIS 로그 메트릭 필터에 동일한 네임스페이스를 사용하는 경우, 모든 CIS Benchmark 메트릭이 함께 그룹화됩니다.

   c. 메트릭 이름에 메트릭의 이름을 입력합니다. 메트릭의 이름을 기억하세요. 경보를 만들 때 메트릭를 선택해야 합니다.

   d. 메트릭 값에 **`1`**를 입력합니다.

   e. 다음을 선택합니다.
7. 검토 및 생성에서 새로운 메트릭 필터에 대해 제공한 정보를 확인합니다. 그런 다음 메트릭 필터 생성을 선택합니다.
8. 탐색 창에서 로그 그룹을 선택한 다음 메트릭 필터에서 생성한 필터를 선택합니다.
9. 필터 확인란을 선택합니다. 경보 생성을 선택하세요.
10. 메트릭 및 조건 지정에서 다음을 수행합니다.

    a. 조건의 임계값에서 정적을 선택합니다.

b. 경보 조건 정의에서 크거나/같음을 선택합니다.

c. 임계값 정의에는 **1**을 입력합니다.

d. 다음을 선택합니다.

11. 작업 구성에서 다음 작업을 수행합니다.

a. 경보 상태 트리거에서 경보를 선택합니다.

b. SNS 주제 선택에서 기존 SNS 주제 선택을 선택합니다.

c. 알림 보내기에 이전 절차에서 생성한 SNS 주제의 이름을 입력합니다.

d. 다음을 선택합니다.

12. 이름 및 설명 추가에서 경보에 대한 이름 및 설명을 입력합니다(예: **CIS-1.1-RootAccountUsage**). 그리고 다음을 선택합니다.

13. 미리 보기 및 생성에서 경보 구성을 검토하세요. 그런 다음 경보 생성을 선택합니다.

[IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.

관련 요구 사항: 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(10), NIST.800-53.r5 AC-6(2), 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, NIST.800-171.r2 3.3.8, NIST.800-171.r2 3.3.9, NIST.800-171.r2 3.13.3, NIST.800-171.r2 3.13.4

범주: 감지 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::IAM::Policy`

AWS Config 규칙: `iam-policy-no-statements-with-full-access`

스케줄 유형: 변경이 트리거됨

파라미터:

- `excludePermissionBoundaryPolicy`: `True`(사용자 지정할 수 없음)

이 제어는 생성한 IAM ID 기반 정책에 * 와일드카드를 사용하여 모든 서비스의 모든 작업에 대한 권한을 부여하는 Allow 문이 있는지 확인합니다. 정책 문에 `"Effect": "Allow"`과 `"Action": "Service:*"`가 포함된 경우, 제어가 실패합니다.

예를 들어, 정책의 다음 문으로 인해 조사 결과가 실패합니다.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:*",
  "Resource": "*"
}
```

"Effect": "Allow"와 "NotAction": "*service*:*"를 함께 사용하는 경우에도 제어가 실패합니다. 이 경우 NotAction 요소는에 지정된 작업을 AWS 서비스제외하고의 모든 작업에 대한 액세스를 제공합니다NotAction.

이 제어는 고객 관리형 IAM 정책에만 적용됩니다. AWS에서 관리하는 IAM 정책에는 적용되지 않습니다.

권한을 할당할 때는 IAM 정책에서 허용되는 IAM 작업의 범위를 지정하는 AWS 서비스것이 중요합니다. IAM 작업은 필요한 작업으로만 제한해야 합니다. 이렇게 하면 최소 권한 권한을 프로비저닝할 수 있습니다. 권한이 과도하게 부여된 정책은 권한이 필요하지 않은 IAM 보안 주체에 정책이 연결된 경우, 권한 상승으로 이어질 수 있습니다.

경우에 따라 DescribeFlowLogs 및 DescribeAvailabilityZones와 같이 접두사가 비슷한 IAM 작업을 허용할 수 있습니다. 이러한 승인된 경우에는 접미사가 붙은 와일드카드를 일반 접두사에 추가할 수 있습니다. 예제: ec2:Describe*.

접두사가 붙은 와일드카드와 함께 접두사가 붙은 IAM 작업을 사용하면 이 제어가 통과됩니다. 예를 들어, 정책의 다음 문으로 인해 조사 결과가 통과합니다.

```
"Statement": [
{
  "Sid": "EC2-Wildcard",
  "Effect": "Allow",
  "Action": "ec2:Describe*",
  "Resource": "*"
}
```

이러한 방식으로 관련 IAM 작업을 그룹화하면 IAM 정책 크기 제한을 초과하는 것을 방지할 수도 있습니다.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서는 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

이 문제를 해결하려면 전체 '*' 관리 권한을 허용하지 않도록 IAM 정책을 업데이트하세요. IAM 정책 편집에 대한 자세한 내용은 IAM 사용자 설명서의 IAM 정책 편집을 참조하세요.

[IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.11, CIS AWS파운데이션 벤치마크 v3.0.0/1.12, CIS AWS파운데이션 벤치마크 v1.4.0/1.12, NIST.800-171.r2 3.1.2

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::User`

AWS Config규칙: `iam-user-unused-credentials-check`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 IAM 사용자가 45일 이상 사용하지 않은 암호 또는 활성 액세스 키를 가지고 있는지 확인합니다. 이를 위해 AWS Config규칙의 `maxCredentialUsageAge` 파라미터가 45 이상인지 확인합니다.

사용자는 암호 또는 액세스 키와 같은 다양한 유형의 자격 증명을 사용하여 AWS리소스에 액세스할 수 있습니다.

CIS에서는 45일 이상 사용되지 않은 모든 자격 증명을 제거하거나 비활성화할 것을 권장합니다. 불필요한 보안 인증을 비활성화하거나 제거하면 침해되거나 버려진 계정과 연결된 보안 인증이 사용될 가능성이 줄어듭니다.

이 제어의 AWS Config규칙은 `GetCredentialReport` 및 `GenerateCredentialReport` API 작업을 사용하며,이 작업은 4시간마다만 업데이트됩니다. IAM 사용자 변경 내용이 이 제어에 표시되는 데 최대 4시간이 걸릴 수 있습니다.

> **Note**
>
> AWS Config는 Security Hub CSPM을 사용하는 모든 리전에서 활성화되어야 합니다. 하지만 단일 리전에서 글로벌 리소스 기록을 활성화할 수 있습니다. 단일 리전에서만 글로벌 리소스를 기록하는 경우, 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 이 제어를 비활성화할 수 있습니다.

문제 해결

IAM 콘솔에서 사용자 정보를 보면 액세스 키 사용 기간, 비밀번호 사용 기간, 마지막 활동 열이 표시됩니다. 이 열 중 어느 하나라도 값이 45일보다 큰 경우, 해당 사용자의 보안 인증을 비활성화하세요.

또한 보안 인증 보고서를 사용해 사용자를 모니터링하고 45일 이상 활동이 없는 사용자를 식별할 수 있습니다. IAM 콘솔에서 `.csv` 형식으로 된 보안 인증 정보 보고서를 다운로드할 수 있습니다.

비활성 계정이나 사용하지 않는 보안 인증 정보를 식별한 후에는 비활성화하세요. 자세한 지침은 IAM 사용자 설명서의 IAM 사용자 암호 생성, 변경 또는 삭제(콘솔)를 참조하세요.

[IAM.23] IAM Access Analyzer 분석기에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::AccessAnalyzer::Analyzer`

AWS Config규칙: `tagged-accessanalyzer-analyzer` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS Identity and Access Management Access Analyzer(IAM Access Analyzer)에서 관리하는 분석기에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 분석기에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 분석기에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

분석기에 태그를 추가하려면 AWS IAM Access Analyzer API 참조의 TagResource 섹션을 참조하세요.

[IAM.24] IAM 역할에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::IAM::Role`

AWS Config규칙: `tagged-iam-role` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS Identity and Access Management(IAM) 역할에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 역할에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 역할에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

IAM 역할에 태그를 추가하려면 IAM 사용자 설명서의 IAM 리소스 태그 지정을 참조하세요.

[IAM.25] IAM 사용자에게 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::IAM::User`

AWS Config규칙: `tagged-iam-user` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS Identity and Access Management(IAM) 사용자에게 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 사용자에게 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 사용자에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

IAM 사용자에게 태그를 추가하려면 IAM 사용자 설명서의 IAM 리소스 태그 지정을 참조하세요.

[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.18, CIS AWS파운데이션 벤치마크 v3.0.0/1.19

범주: 식별 > 규정 준수

심각도: 중간

리소스 유형: `AWS::IAM::ServerCertificate`

AWS Config규칙: `iam-server-certificate-expiration-check`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 IAM에서 관리되는 활성 SSL/TLS 서버 인증서가 만료되었는지 확인합니다. 만료된 SSL/TLS 서버 인증서가 제거되지 않으면 제어가 실패합니다.

에서 웹 사이트 또는 애플리케이션에 대한 HTTPS 연결을 활성화하려면 SSL/TLS 서버 인증서가 AWS 필요합니다. IAM 또는 AWS Certificate Manager(ACM)을 사용하여 서버 인증서를 저장하고 배포할 수 있습니다. ACM에서 지원하지 않는에서 HTTPS 연결을 지원해야 AWS 리전하는 경우에만 IAM을 인증서 관리자로 사용합니다. IAM은 프라이빗 키를 안전하게 암호화하고 암호화된 버전을 IAM SSL 인증서 스토리지에 저장합니다. IAM은 모든 리전에서 서버 인증서 배포를 지원하지만와 함께 사용하려면 외부 공급자로부터 인증서를 받아야 합니다AWS. ACM 인증서는 IAM에 업로드할 수 없습니다. 또한 IAM 콘솔에서 인증서를 관리할 수 없습니다. 만료된 SSL/TLS 인증서를 제거하면 잘못된 인증서가 리소스에 실수로 배포되어 기본 애플리케이션 또는 웹사이트의 신뢰성이 손상될 위험이 없습니다.

문제 해결

IAM에서 서버 인증서를 제거하려면 IAM 사용자 설명서의 IAM에서 서버 인증서 관리를 참조하세요.

[IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.21, CIS AWS파운데이션 벤치마크 v3.0.0/1.22

범주: 보호 > 보안 액세스 관리 > 보안 IAM 정책

심각도: 중간

리소스 유형: `AWS::IAM::Role`, `AWS::IAM::User`, `AWS::IAM::Group`

AWS Config규칙: `iam-policy-blacklisted-check`

스케줄 유형: 변경이 트리거됨

파라미터:

- "policyArns": "arn:aws:iam::aws:policy/AWSCloudShellFullAccess,arn:aws-cn:iam::aws:policy/AWSCloudShellFullAccess, arn:aws-us-gov:iam::aws:policy/AWSCloudShellFullAccess"

이 제어는 IAM 자격 증명(사용자, 역할 또는 그룹)에 AWS관리형 정책이 `AWSCloudShellFullAccess` 연결되어 있는지 확인합니다. IAM ID에 `AWSCloudShellFullAccess` 정책이 연결된 경우, 제어가 실패합니다.

AWS CloudShell는 CLI 명령을 실행할 수 있는 편리한 방법을 제공합니다AWS 서비스. AWS관리형 정책은 사용자의 로컬 시스템과 CloudShell 환경 간에 파일 업로드 및 다운로드 기능을 허용하는 CloudShell에 대한 전체 액세스를 `AWSCloudShellFullAccess` 제공합니다. CloudShell 환경 내에서 사용자는 sudo 권한을 가지며 인터넷에 액세스할 수 있습니다. 따라서 이 관리형 정책을 IAM ID에 연결하면 File Transfer 소프트웨어를 설치하고 CloudShell에서 외부 인터넷 서버로 데이터를 이동할 수 있습니다. 최소 권한 원칙을 따르고 IAM 자격 증명에 더 좁은 권한을 연결하는 것이 좋습니다.

문제 해결

IAM ID에서 `AWSCloudShellFullAccess` 정책을 분리하려면 IAM 사용자 설명서의 IAM ID 권한 추가 및 제거를 참조하세요.

[IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/1.19, CIS AWS파운데이션 벤치마크 v3.0.0/1.20

범주: 감지 > 감지 서비스 > 권한 있는 사용 모니터링

심각도: 높음

리소스 유형: `AWS::AccessAnalyzer::Analyzer`

AWS Config규칙: `iam-external-access-analyzer-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는에 IAM Access Analyzer 외부 액세스 분석기AWS 계정가 활성화되어 있는지 확인합니다. 계정에 현재 선택한 AWS 리전에서 활성화된 외부 액세스 분석기가 없는 경우, 제어가 실패합니다.

IAM Access Analyzer 외부 액세스 분석기를 사용하면 Amazon Simple Storage Service(Amazon S3) 버킷 또는 IAM 역할과 같은 외부 엔터티와 공유되는 리소스를 식별할 수 있습니다. 이를 통해 리소스 및 데이터에 대한 의도치 않은 액세스를 식별할 수 있습니다. IAM Access Analyzer는 리전이며 각 리전에서 활성화되어야 합니다. 외부 보안 주체와 공유되는 리소스를 식별하기 위해 액세스 분석기는 로직 기반 추론을 사용하여 AWS환경의 리소스 기반 정책을 분석합니다. 외부 액세스 분석기를 생성할 때 전체 조직 또는 개별 계정에 대한 분석기를 생성하고 활성화할 수 있습니다.

> **Note**
>
> 계정이에 있는 조직의 일부인 경우 AWS Organizations이 제어는 조직을 신뢰 영역으로 지정하고 현재 리전의 조직에 대해 활성화된 외부 액세스 분석기를 고려하지 않습니다. 조직이 이러한 유형의 구성을 사용하는 경우 해당 리전에서 조직의 개별 멤버 계정에 대해 이 제어를 비활성화하는 것이 좋습니다.

문제 해결

특정 리전에서 외부 액세스 분석기를 활성화하는 방법에 대한 자세한 내용은 IAM 사용자 설명서의 IAM Access Analyzer 활성화를 참조하세요. 리소스에 대한 액세스 권한을 모니터링하려는 각 리전에서 분석기를 생성해야 합니다.

## Amazon Inspector에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Inspector 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/11.3.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `inspector-ec2-scan-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Inspector EC2 스캔이 활성화되어 있는지 확인합니다. 독립형 계정의 경우, Amazon Inspector EC2 스캔이 계정에서 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 Amazon Inspector 관리자 계정과 모든 멤버 계정에 EC2 스캔이 활성화되지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 Amazon Inspector 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 EC2 스캔 기능을 활성화하거나 비활성화할 수 있습니다. Amazon Inspector 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 관리자에게 Amazon Inspector EC2 스캔이 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 Amazon Inspector 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

Amazon Inspector EC2 스캔은 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 메타데이터를 추출한 다음, 이 메타데이터를 보안 권고에서 수집한 규칙과 비교하여 조사 결과를 생성합니다. Amazon Inspector는 인스턴스에서 패키지 취약성과 네트워크 연결 문제를 스캔합니다. SSM 에이전트 없이 스캔할 수 있는 운영 체제를 비롯하여 지원되는 운영 체제에 대한 자세한 내용은 지원되는 운영 시스템: Amazon EC2 스캔을 참조하세요.

문제 해결

Amazon Inspector EC2 스캔을 활성화하려면 Amazon Inspector 사용 설명서의 스캔 활성화를 참조하세요.

[Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/11.3.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `inspector-ecr-scan-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Inspector ECR 스캔이 활성화되어 있는지 확인합니다. 독립형 계정의 경우, Amazon Inspector ECR 스캔이 계정에서 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 Amazon Inspector 관리자 계정과 모든 멤버 계정에 ECR 스캔이 활성화되지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 Amazon Inspector 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 ECR 스캔 기능을 활성화하거나 비활성화할 수 있습니다. Amazon Inspector 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 관리자에게 Amazon Inspector ECR 스캔이 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 Amazon Inspector 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

Amazon Inspector는 Amazon Elastic Container Registry (Amazon ECR)에 저장된 컨테이너 이미지에 소프트웨어 취약성이 있는지 스캔하여 패키지 취약성 조사 결과를 생성합니다. Amazon ECR에 대한 Amazon Inspector 스캔을 활성화할 때 프라이빗 레지스트리의 기본 스캔 서비스로 Amazon Inspector를 설정하세요. 그러면 Amazon ECR에서 무료로 제공하는 기본 스캔이 Amazon Inspector를 통해 제공되고 요금이 청구되는 고급 스캔으로 대체됩니다. 고급 스캔 기능을 사용하면 레지스트리 수준에서 운영 체제 및 프로그래밍 언어 패키지 모두에 대한 취약성 스캔의 이점을 누릴 수 있습니다. 이미지의 각 계층에 대해 이미지 수준에서 고급 스캔을 사용하여 발견된 조사 결과는 Amazon ECR 콘솔에서 검토할 수 있습니다. 또한 AWS Security Hub CSPM및 Amazon EventBridge를 포함하여 기본 스캔 결과에 사용할 수 없는 다른 서비스에서 이러한 결과를 검토하고 작업할 수 있습니다.

문제 해결

Amazon Inspector ECR 스캔을 활성화하려면 Amazon Inspector 사용 설명서의 스캔 활성화를 참조하세요.

[Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `inspector-lambda-code-scan-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Inspector Lambda 코드 스캔이 활성화되어 있는지 확인합니다. 독립형 계정의 경우, Amazon Inspector Lambda 코드 스캔이 계정에서 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 Amazon Inspector 관리자 계정과 모든 멤버 계정에 Lambda 코드 스캔이 활성화되지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 Amazon Inspector 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 Lambda 코드 스캔 기능을 활성화하거나 비활성화할 수 있습니다. Amazon Inspector 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 관리자에게 Amazon Inspector Lambda 코드 스캔이 활성화되지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 Amazon Inspector 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

Amazon Inspector Lambda 코드 스캔은 AWS보안 모범 사례에 따라 AWS Lambda함수 내의 사용자 지정 애플리케이션 코드에서 코드 취약성을 스캔합니다. Lambda 코드 스캔으로 코드에서 주입 결함, 데이터 유출, 취약한 암호화 또는 누락된 암호화를 탐지할 수 있습니다. 이 기능은 특정 AWS 리전에서만 사용할 수 있습니다. Lambda 코드 스캔은 Lambda 표준 스캔과 함께 활성화할 수 있습니다 ([Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다. 참조).

문제 해결

Amazon Inspector Lambda 코드 스캔을 활성화하려면 Amazon Inspector 사용 설명서의 스캔 활성화를 참조하세요.

[Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/6.2.4, PCI DSS v4.0.1/6.3.1

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `inspector-lambda-standard-scan-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Inspector Lambda 표준 스캔이 활성화되어 있는지 확인합니다. 독립형 계정의 경우, Amazon Inspector Lambda 표준 스캔이 계정에서 비활성화되면 제어가 실패합니다. 다중 계정 환경에서는 위임된 Amazon Inspector 관리자 계정과 모든 멤버 계정에 Lambda 표준 스캔이 활성화되지 않은 경우, 제어가 실패합니다.

다중 계정 환경에서 제어는 위임된 Amazon Inspector 관리자 계정에서만 조사 결과를 생성합니다. 위임된 관리자만 조직의 멤버 계정에 대해 Lambda 표준 스캔 기능을 활성화하거나 비활성화할 수 있습니다. Amazon Inspector 멤버 계정은 계정 내에서 이 구성을 수정할 수 없습니다. 이 제어는 위임된 관리자에게 Amazon Inspector Lambda 표준 스캔을 활성화하지 않은 일시 중지된 멤버 계정이 있는 경우, `FAILED` 조사 결과를 생성합니다. `PASSED` 조사 결과를 받으려면 위임된 관리자가 Amazon Inspector 에서 이러한 일시 중지된 계정의 연결을 해제해야 합니다.

Amazon Inspector Lambda 표준 스캔은 AWS Lambda함수 코드 및 계층에 추가하는 애플리케이션 패키지 종속성의 소프트웨어 취약성을 식별합니다. Amazon Inspector에서 Lambda 함수 애플리케이션 패키지 종속성의 취약성을 탐지한 경우, Amazon Inspector는 상세한 `Package Vulnerability` 유형의 조사 결과를 생성합니다. Lambda 코드 스캔은 Lambda 표준 스캔과 함께 활성화할 수 있습니다 ([Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다. 참조).

문제 해결

Amazon Inspector Lambda 표준 스캔을 활성화하려면 Amazon Inspector 사용 설명서의 스캔 활성화를 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS IoT

이러한 AWS Security Hub CSPM제어는 AWS IoT서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::SecurityProfile`

AWS Config규칙: `tagged-iot-securityprofile` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS IoT Device Defender보안 프로필에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 보안 프로파일에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 보안 프로파일에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS IoT Device Defender보안 프로필에 태그를 추가하려면 AWS IoT개발자 안내서의 AWS IoT리소스 태그 지정을 참조하세요.

[IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::MitigationAction`

AWS Config규칙: `tagged-iot-mitigationaction` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS IoT Core완화 작업에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 완화 작업에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 서비스에 완화 작업에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수

있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS IoT Core완화 작업에 태그를 추가하려면 AWS IoT개발자 안내서의 AWS IoT리소스 태그 지정을 참조하세요.

[IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::Dimension`

AWS Config규칙: `tagged-iot-dimension` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS IoT Core차원에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 차원에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가

없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 볼륨에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS IoT Core차원에 태그를 추가하려면 AWS IoT개발자 안내서의 AWS IoT리소스 태그 지정을 참조하세요.

[IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::Authorizer`

AWS Config규칙: `tagged-iot-authorizer` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS IoT Core권한 부여자에게 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 권한 부여자에게 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 권한 부여자에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS IoT Core권한 부여자에 태그를 추가하려면 AWS IoT개발자 안내서의 AWS IoT리소스 태그 지정을 참조하세요.

[IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::RoleAlias`

AWS Config규칙: `tagged-iot-rolealias` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS IoT Core역할 별칭에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 역할 별칭에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 역할 별칭에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS IoT Core역할 별칭에 태그를 추가하려면 AWS IoT개발자 안내서의 AWS IoT리소스 태그 지정을 참조하세요.

[IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoT::Policy`

AWS Config규칙: `tagged-iot-policy` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS IoT Core정책에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 정책에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 정책에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수

있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

AWS IoT Core정책에 태그를 추가하려면 AWS IoT개발자 안내서의 AWS IoT리소스 태그 지정을 참조하세요.

## AWSIoT SiteWise에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWSIoT SiteWise 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTSiteWise::AssetModel`

AWS Config 규칙: `iotsitewise-asset-model-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 AWSIoT SiteWise 자산 모델에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 자산 모델에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 자산 모델에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT SiteWise 자산 모델에 태그를 추가하려면 AWS IoT SiteWise사용 설명서의 AWS IoT SiteWise리소스 태그 지정을 참조하세요.

[IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTSiteWise::Dashboard`

AWS Config 규칙: `iotsitewise-dashboard-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT SiteWise 대시보드에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 대시보드에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 대시보드에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT SiteWise 대시보드에 태그를 추가하려면 AWS IoT SiteWise사용 설명서의 AWS IoT SiteWise리소스 태그 지정을 참조하세요.

[IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTSiteWise::Gateway`

AWS Config 규칙: `iotsitewise-gateway-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT SiteWise 게이트웨이에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 게이트웨이에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 게이트웨이에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수

있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT SiteWise 게이트웨이에 태그를 추가하려면 AWS IoT SiteWise사용 설명서의 AWS IoT SiteWise리소스 태그 지정을 참조하세요.

[IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTSiteWise::Portal`

AWS Config 규칙: `iotsitewise-portal-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT SiteWise 포털에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 포털에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가

없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 포털에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT SiteWise 포털에 태그를 추가하려면 AWS IoT SiteWise사용 설명서의 AWS IoT SiteWise리소스 태그 지정을 참조하세요.

[IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTSiteWise::Project`

AWS Config 규칙: `iotsitewise-project-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT SiteWise 프로젝트에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 프로젝트에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 프로젝트에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT SiteWise 프로젝트에 태그를 추가하려면 AWS IoT SiteWise사용 설명서의 AWS IoT SiteWise리소스 태그 지정을 참조하세요.

## AWSIoT TwinMaker에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWSIoT TwinMaker 서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTTwinMaker::SyncJob`

AWS Config 규칙: `iottwinmaker-sync-job-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT TwinMaker 동기화 작업에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 동기화 작업에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 동기화 작업에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을

정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT TwinMaker 동기화 작업에 태그를 추가하려면 AWS IoT TwinMaker사용 설명서TagResource의 섹션을 참조하세요.

[IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTTwinMaker::Workspace`

AWS Config 규칙: `iottwinmaker-workspace-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT TwinMaker 워크스페이스에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 워크스페이스에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 워크스페이스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT TwinMaker 워크스페이스에 태그를 추가하려면 AWS IoT TwinMaker사용 설명서TagResource의 섹션을 참조하세요.

[IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTTwinMaker::Scene`

AWS Config 규칙: `iottwinmaker-scene-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT TwinMaker 장면에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 장면에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 장면에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT TwinMaker 장면에 태그를 추가하려면 AWS IoT TwinMaker사용 설명서TagResource의 섹션을 참조하세요.

[IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTTwinMaker::Entity`

AWS Config 규칙: `iottwinmaker-entity-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT TwinMaker 엔터티에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 엔터티에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 엔터티에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT TwinMaker 엔터티에 태그를 추가하려면 AWS IoT TwinMaker사용 설명서TagResource의 섹션을 참조하세요.

## AWSIoT Wireless에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWSIoT Wireless 서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTWireless::MulticastGroup`

AWS Config 규칙: `iotwireless-multicast-group-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT Wireless 멀티캐스트 그룹에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 멀티캐스트 그룹에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 멀티캐스트 그룹에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT Wireless 멀티캐스트 그룹에 태그를 추가하려면 AWS IoT 무선개발자 안내서의 AWS IoT 무선리소스 태그 지정을 참조하세요.

[IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTWireless::ServiceProfile`

AWS Config 규칙: `iotwireless-service-profile-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT Wireless 서비스 프로파일에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 서비스 프로파일에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 서비스 프로파일에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT Wireless 서비스 프로파일에 태그를 추가하려면 AWS IoT 무선개발자 안내서의 AWS IoT 무선리소스 태그 지정을 참조하세요.

[IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IoTWireless::FuotaTask`

AWS Config 규칙: `iotwireless-fuota-task-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSIoT Wireless 펌웨어 over-the-air 업데이트(FUOTA) 작업에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. FUOTA 태스크에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 FUOTA 태스크에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWSIoT Wireless FUOTA 작업에 태그를 추가하려면 AWS IoT 무선개발자 안내서의 AWS IoT 무선리소스 태그 지정을 참조하세요.

## Amazon IVS에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Interactive Video Service(IVS) 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IVS::PlaybackKeyPair`

AWS Config 규칙: `ivs-playback-key-pair-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon IVS 재생 키 페어에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 재생 키 페어에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 재생 키 페어에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

IVS 재생 키 페어에 태그를 추가하려면 Amazon IVS Real-Time Streaming API 참조의 TagResource를 참조하세요.

[IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IVS::RecordingConfiguration`

AWS Config 규칙: `ivs-recording configuration-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon IVS 레코딩 구성에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 레코딩 구성에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 레코딩 구성에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

IVS 레코딩 구성에 태그를 추가하려면 Amazon IVS Real-Time Streaming API 참조의 TagResource를 참조하세요.

[IVS.3] IVS 채널에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::IVS::Channel`

AWS Config 규칙: `ivs-channel-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon IVS 채널에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 채널에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 채널에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계

할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

IVS 채널에 태그를 추가하려면 Amazon IVS Real-Time Streaming API 참조의 TagResource를 참조하세요.

## Amazon Keyspaces에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Keyspaces 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Cassandra::Keyspace`

AWS Config 규칙: `cassandra-keyspace-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon Keyspaces 키스페이스에 파라미터 `requiredKeyTags`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 키스페이스에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 키스페이스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

Amazon Keyspaces 키스페이스에 태그를 추가하려면 Amazon Keyspaces 개발자 안내서의 키스페이스에 태그 추가를 참조하세요.

## Kinesis에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Kinesis 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Kinesis::Stream`

AWS Config 규칙: kinesis-stream-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Kinesis Data Streams가 서버 측 암호화를 통해 저장 시 암호화되는지 확인합니다. Kinesis 스트림이 서버 측 암호화를 통해 저장 시 암호화되지 않으면 이 제어가 실패합니다.

서버 측 암호화는 Amazon Kinesis Data Streams의 기능으로, 데이터를 저장하기 전에 AWS KMS key를 사용하여 자동으로 암호화합니다. 데이터는 Kinesis 스트림 스토리지 계층에 기록되기 전에 암호화되고, 스토리지에서 검색된 후에는 해독됩니다. 결과적으로 데이터는 Amazon Kinesis Data Streams 서비스 내에서 암호화됩니다.

문제 해결

Kinesis 스트림의 서버 측 암호화를 활성화에 대한 자세한 내용은 Amazon Kinesis 개발자 안내서의 서버 측 암호화를 시작하려면 어떻게 해야 합니까?를 참조하세요.

[Kinesis.2] Kinesis 스트림에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Kinesis::Stream`

AWS Config규칙: `tagged-kinesis-stream` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Kinesis Data Streams에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 데이터 스트림에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 데이터 스트림에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Kinesis 데이터 스트림에 태그를 추가하려면 Amazon Kinesis 개발자 안내서의 Amazon Kinesis Data Streams에서 스트림 태그 지정을 참조하세요.

[Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.

심각도: 중간

리소스 유형: `AWS::Kinesis::Stream`

AWS Config 규칙: kinesis-stream-backup-retention-check

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `minimumBackupRetentionPeriod` | 데이터를 보존해야 하는 최소 시간입니다. | 문자열 | 24~8760 | 168 |

이 제어는 Amazon Kinesis Data Streams의 백업 보존 기간이 지정된 기간 이상인지 여부를 확인합니다. 백업 보존 기간이 지정된 기간 미만인 경우, 제어가 실패합니다. 데이터 보존 기간 동안 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 168시간을 사용합니다.

Kinesis 데이터 스트림은 실시간으로 읽고 쓸 수 있는 정렬된 순서의 데이터 레코드입니다. 따라서 데이터 레코드는 스트림의 샤드에 일시적으로 저장됩니다. 데이터가 추가된 시점부터 더 이상 액세스할 수 없는 시점까지의 기간을 보관 기간이라고 합니다. 보존 기간이 감소되면 Kinesis Data Streams는 새로운 보존 기간보다 이전인 레코드를 즉시 액세스할 수 없도록 합니다. 예를 들어, 보존 기간을 24시간에서 48시간으로 변경하면 23시간 55분 전에 스트림에 추가된 레코드는 24시간 후에도 계속 사용할 수 있습니다.

문제 해결

Kinesis Data Streams의 백업 보존 기간을 변경하려면 Amazon Kinesis Data Streams 개발자 안내서의 데이터 보존 기간 변경을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS KMS

이러한 AWS Security Hub CSPM제어는 AWS Key Management Service(AWS KMS) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::IAM::Policy`

AWS Config 규칙: iam-customer-policy-blocked-kms-actions

스케줄 유형: 변경이 트리거됨

파라미터:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(사용자 지정할 수 없음)
- `excludePermissionBoundaryPolicy: True`(사용자 지정할 수 없음)

IAM 고객 관리형 정책의 기본 버전이 보안 주체가 모든 리소스에서 AWS KMS복호화 작업을 사용하도록 허용하는지 확인합니다. 모든 KMS 키에 대해 `kms:Decrypt` 또는 `kms:ReEncryptFrom` 작업을 허용할 만큼 정책이 공개되어 있으면 제어가 실패합니다.

제어는 리소스 요소의 KMS 키만 검사하고 정책의 조건 요소에 있는 조건은 고려하지 않습니다. 또한 제어는 연결된 고객 관리형 정책과 연결되지 않은 고객 관리형 정책을 모두 평가합니다. 인라인 정책 또는 AWS관리형 정책은 확인하지 않습니다.

AWS KMS를 사용하면 KMS 키를 사용할 수 있는 사용자를 제어하고 암호화된 데이터에 액세스할 수 있습니다. IAM 정책은 ID(사용자, 그룹 또는 역할)가 어떤 리소스에 대해 어떤 작업을 수행할 수 있는지 정의합니다. 보안 모범 사례에 따라 최소 권한을 허용하는 것이 AWS좋습니다. 즉, ID에 `kms:Decrypt` 또는 `kms:ReEncryptFrom` 권한만 부여하고 작업을 수행하는 데 필요한 키에 대해서만 부여해야 합니다. 그렇지 않으면 사용자가 데이터에 적합하지 않은 키를 사용할 수 있습니다.

모든 키에 대한 권한을 부여하는 대신 사용자가 암호화된 데이터에 액세스하는 데 필요한 최소 키 세트를 결정합니다. 그런 다음 사용자가 해당 키만 사용하도록 허용하는 정책을 설계합니다. 예를 들어, 모든 KMS 키에 대한 `kms:Decrypt` 권한을 허용하지 마세요. 대신 계정의 특정 리전에 있는 키에만 `kms:Decrypt`를 허용하세요. 최소 권한 원칙을 채택하면 데이터가 의도하지 않게 공개될 위험을 줄일 수 있습니다.

문제 해결

IAM 고객 관리형 정책을 수정하려면 IAM 사용자 설명서의 고객 관리형 정책 편집을 참조하세요. 정책을 편집할 때 암호 해독 작업을 허용하려는 특정 키의 Amazon 리소스 이름(ARN)을 `Resource` 필드에 제공합니다.

[KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

AWS Config 규칙: iam-inline-policy-blocked-kms-actions

스케줄 유형: 변경이 트리거됨

파라미터:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt`(사용자 지정할 수 없음)

이 제어는 IAM 자격 증명(역할, 사용자 또는 그룹)에 포함된 인라인 정책이 모든 KMS 키에 대한 AWS KMS복호화 및 재암호화 작업을 허용하는지 확인합니다. 모든 KMS 키에 대해 `kms:Decrypt` 또는 `kms:ReEncryptFrom` 작업을 허용할 만큼 정책이 공개되어 있으면 제어가 실패합니다.

제어는 리소스 요소의 KMS 키만 검사하고 정책의 조건 요소에 있는 조건은 고려하지 않습니다.

AWS KMS를 사용하면 KMS 키를 사용할 수 있는 사용자를 제어하고 암호화된 데이터에 액세스할 수 있습니다. IAM 정책은 ID(사용자, 그룹 또는 역할)가 어떤 리소스에 대해 어떤 작업을 수행할 수 있는지 정의합니다. 보안 모범 사례에 따라 최소 권한을 허용하는 것이 AWS좋습니다. 즉, 필요한 권한과 작업을 수행하는 데 필요한 키만 ID에 부여해야 합니다. 그렇지 않으면 사용자가 데이터에 적합하지 않은 키를 사용할 수 있습니다.

모든 키에 권한을 부여하는 대신 사용자가 암호화된 데이터에 액세스하는 데 필요한 최소 키 세트를 결정하세요. 그런 다음 사용자가 해당 키만 사용하도록 허용하는 정책을 설계합니다. 예를 들어, 모든 KMS 키에 대한 `kms:Decrypt` 권한을 허용하지 마세요. 대신 계정에 대한 특정 리전의 특정 키에 대해서만 권한을 허용하세요. 최소 권한 원칙을 채택하면 데이터가 의도하지 않게 공개될 위험을 줄일 수 있습니다.

문제 해결

IAM 인라인 정책을 수정하려면 IAM 사용자 설명서의 인라인 정책 편집을 참조하세요. 정책을 편집할 때 암호 해독 작업을 허용하려는 특정 키의 Amazon 리소스 이름(ARN)을 `Resource` 필드에 제공합니다.

[KMS.3] 실수로 삭제해서는 AWS KMS keys안 됩니다.

관련 요구 사항: NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12(2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 심각

리소스 유형: `AWS::KMS::Key`

AWS Config규칙: `kms-cmk-not-scheduled-for-deletion-2` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 KMS 키가 삭제되도록 예약되어 있는지 여부를 확인합니다. KMS 키 삭제가 예약된 경우, 제어가 실패합니다.

KMS 키는 일단 삭제되면 복구할 수 없습니다. KMS 키를 삭제하면 KMS 키로 암호화된 데이터도 영구적으로 복구할 수 없습니다. 삭제될 예정인 KMS 키로 의미 있는 데이터를 암호화한 경우, 의도적으로

암호화 삭제를 수행하지 않는 한 데이터를 해독하거나 새로운 KMS 키로 데이터를 다시 암호화하는 것을 고려해 보세요.

KMS 키 삭제가 예약되면 오류로 예약된 경우, 삭제를 되돌릴 수 있는 시간을 확보하기 위해 필수 대기 기간이 적용됩니다. 기본 대기 기간은 30일이지만 KMS 키 삭제가 예정된 경우, 짧게는 7일로 줄일 수 있습니다. 대기 기간 동안에는 예약된 삭제를 취소할 수 있으며 KMS 키는 삭제되지 않습니다.

KMS 키 삭제에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 KMS 키 삭제를 참조하세요.

문제 해결

예약된 KMS 키 삭제를 취소하려면 AWS Key Management Service 개발자 안내서의 키 삭제 예약 및 취소(콘솔) 아래의 키 삭제를 취소하려면을 참조하세요.

[KMS.4]AWS KMS키 교체를 활성화해야 합니다.

관련 요구 사항: CIS AWS파운데이션 벤치마크 v5.0.0/3.6, CIS AWS파운데이션 벤치마크 v3.0.0/3.6, CIS AWS파운데이션 벤치마크 v1.4.0/3.8, CIS AWS파운데이션 벤치마크 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

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::KMS::Key`

AWS Config 규칙: cmk-backing-key-rotation-enabled

스케줄 유형: 주기적

파라미터: 없음

AWS KMS를 사용하면 고객이에 저장된 키 구성 요소이며 KMS 키의 키 ID에 AWS KMS연결된 지원 키를 교체할 수 있습니다. 이 백업 키는 암호화, 해독 등 암호화 작업을 수행하는 데 사용됩니다. 자동화된 키 교체는 암호화된 데이터의 해독이 투명하게 이루어질 수 있도록 하기 위해 현재 모든 이전 버전의 백업 키를 유지합니다.

CIS에서는 KMS 키 순환을 활성화할 것을 권장합니다. 암호화 키를 교체하면 노출되었을 수 있는 이전 키로 새로운 키로는 암호화된 데이터에 액세스할 수 없으므로 침해된 키가 영향을 미칠 가능성을 줄일 수 있습니다.

문제 해결

KMS 키 교체를 활성화하려면 AWS Key Management Service 개발자 안내서의 자동 키 교체를 활성화 및 비활성화하는 방법을 참조하세요.

[KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::KMS::Key`

AWS Config 규칙: kms-key-policy-no-public-access

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어AWS KMS key는에 공개적으로 액세스할 수 있는지 확인합니다. KMS 키에 공개적으로 액세스할 수 있는 경우, 제어가 실패합니다.

최소 권한 액세스를 구현하는 것은 보안 위험과 오류 또는 악의적 의도의 영향을 줄이는 데 필수적입니다. 에 대한 키 정책이 외부 계정에서 액세스를 AWS KMS key허용하는 경우 타사는 키를 사용하여 데이터를 암호화하고 복호화할 수 있습니다. 이로 인해 내부 또는 외부 위협이 키를 사용하는에서 데이터를 유출AWS 서비스할 수 있습니다.

> **Note**
>
> 또한이 제어는 구성으로 AWS Config인해가 KMS 키의 구성 항목(CI)에 키 정책을 기록하지 못하는 AWS KMS key경우에 대한 `FAILED` 결과를 반환합니다. 가 KMS 키의 CI에 키 정책을 채우AWS Config려면 AWS Config 역할에 GetKeyPolicy API 호출을 사용하여 키 정책을 읽을 수 있는 액세스 권한이 있어야 합니다. 이러한 유형의 `FAILED` 조사 결과를 해결하려면 AWS Config역할이 KMS 키의 키 정책에 대한 읽기 액세스 권한을 갖지 못하게 할 수 있는 정책을 확인합니다. 예를 들어 다음을 확인합니다.
>
> - KMS 키의 키 정책.
> - 계정에 AWS Organizations적용되는의 서비스 제어 정책(SCPs) 및 리소스 제어 정책(RCPs).
> - AWS Config 서비스 연결 AWS Config역할을 사용하지 않는 경우 역할에 대한 권한입니다.

또한 이 제어는 와일드카드 문자 또는 변수를 사용하는 정책 조건을 평가하지 않습니다. PASSED 조사 결과를 생성하려면 키 정책의 조건이 고정 값, 즉 와일드카드 문자 또는 정책 변수를 포함하지 않는 값만 사용해야 합니다. 정책 변수에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 변수 및 태그를 참조하세요.

문제 해결

의 키 정책 업데이트에 대한 자세한 내용은 AWS Key Management Service개발자 안내서의 의 키 정책을AWS KMS AWS KMS key참조하세요.

## 에 대한 Security Hub CSPM 제어 AWS Lambda

이러한 AWS Security Hub CSPM 제어는 AWS Lambda 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: lambda-function-public-access-prohibited

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Lambda 함수 리소스 기반 정책이 계정 외부의 퍼블릭 액세스를 금지하는지 여부를 확인합니다. 퍼블릭 액세스가 허용되면 제어가 실패합니다. Amazon S3에서 Lambda 함수를 호출하고 정책

에 AWS:SourceAccount와 같이 퍼블릭 액세스를 제한하는 조건이 포함되어 있지 않은 경우에도 제어가 실패합니다. 액세스를 더 세분화하려면 버킷 정책에 AWS:SourceAccount와 다른 S3 조건을 함께 사용하는 것이 좋습니다.

> **Note**
>
> 이 제어는 와일드카드 문자 또는 변수를 사용하는 정책 조건을 평가하지 않습니다. PASSED 조사 결과를 생성하려면 Lambda 함수에 대한 정책의 조건이 고정 값, 즉 와일드카드 문자 또는 정책 변수를 포함하지 않는 값만 사용해야 합니다. 정책 변수에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 변수 및 태그를 참조하세요.

Lambda 함수는 의도하지 않은 함수 코드에 접근할 수 있으므로 공개적으로 액세스할 수 없어야 합니다.

문제 해결

이 문제를 해결하려면 함수의 리소스 기반 정책을 업데이트하여 권한을 제거하거나 AWS:SourceAccount 조건을 추가해야 합니다. Lambda API 또는 에서만 리소스 기반 정책을 업데이트할 수 있습니다 AWS CLI.

시작하려면 Lambda 콘솔에서 리소스 기반 정책을 검토하세요. 정책을 공개하는 Principal 필드 값(예: "*" 또는 { "AWS": "*" })이 포함된 정책문을 식별하세요.

콘솔에서는 정책을 편집할 수 없습니다. 함수에서 권한을 제거하려면 AWS CLI에서 remove-permission 명령을 실행합니다.

```
$ aws lambda remove-permission --function-name <function-name> --statement-
id <statement-id>
```

*<function-name>*을 Lambda 함수 이름으로 바꾸고, *<statement-id>*을 제거하려는 문의 문 ID(Sid)로 대체하세요.

[Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 개발

심각도: 중간

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: lambda-function-settings-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `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`(사용자 지정할 수 없음)

이 제어는 AWS Lambda 함수 런타임 설정이 각 언어에서 지원되는 런타임에 대해 설정된 예상 값과 일치하는지 확인합니다. Lambda 함수가 파라미터 섹션에 언급된 지원되는 런타임을 사용하지 않는 경우 제어가 실패합니다. Security Hub CSPM은 패키지 유형이 인 함수를 무시합니다`Image`.

Lambda 런타임은 유지 관리 및 보안 업데이트가 적용되는 운영 체제, 프로그래밍 언어, 소프트웨어 라이브러리의 조합을 기반으로 구축됩니다. 보안 업데이트를 위해 런타임 구성 요소가 더 이상 지원되지 않으면 Lambda는 런타임을 더 이상 사용하지 않습니다. 사용되지 않는 런타임을 사용하는 함수를 만들 수는 없지만 이 함수는 호출 이벤트를 처리하는 데 계속 사용할 수 있습니다. Lambda 함수가 최신 상태이고 더 이상 사용되지 않는 런타임 환경을 사용하지 않는 것이 좋습니다. 지원되는 런타임 목록은 AWS Lambda 개발자 안내서의 Lambda 런타임을 참조하세요.

문제 해결

지원되는 런타임 및 지원 중단 일정에 대한 자세한 내용은 AWS Lambda 개발자 안내서의 런타임 지원 중단 정책을 참조하세요. 런타임을 최신 버전으로 마이그레이션할 때는 해당 언어 게시자의 구문과 지침을 따르세요. 드물게 런타임 버전 비호환성이 발생하는 경우, 워크로드에 영향을 미칠 위험을 줄이기 위해 런타임 업데이트를 적용하는 것이 좋습니다.

[Lambda.3] Lambda 함수는 VPC에 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: lambda-inside-vpc

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Lambda 함수가가상 프라이빗 클라우드(VPC)에 있는지 여부를 확인합니다. Lambda 함수가 VPC에 배포되지 않으면 제어가 실패합니다. Security Hub CSPM은 퍼블릭 연결 가능성을 결정하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다. Lambda@Edge 리소스에 대해 실패한 조사 결과가 표시될 수 있습니다.

VPC에 리소스를 배포하면 네트워크 구성에 대한 보안 및 제어가 강화됩니다. 또한 이러한 배포는 여러 가용 영역에서 확장성과 높은 내결함성을 제공합니다. 다양한 애플리케이션 요구 사항을 충족하도록 VPC 배포를 사용자 지정할 수 있습니다.

문제 해결

VPC의 프라이빗 서브넷에 연결하도록 기존 함수를 구성하려면 AWS Lambda 개발자 안내서의 VPC 액세스 구성을 참조하세요. 고가용성을 위해 최소 두 개의 프라이빗 서브넷을 선택하고 함수의 연결 요구 사항을 충족하는 보안 그룹을 하나 이상 선택하는 것이 좋습니다.

[Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: lambda-vpc-multi-az-check

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `availabilityZones` | 최소 가용 영역의 수 | Enum | `2, 3, 4, 5, 6` | `2` |

이 제어는 Virtual Private Cloud(VPC)에 연결하는 AWS Lambda 함수가 지정된 수 이상의 가용 영역(AZs)에서 작동하는지 확인합니다. 함수가 최소한 지정된 수의 AZ에서 작동하지 않으면 제어가 실패합니다. 최소 AZs 수에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 2개의 AZs 사용합니다.

여러 AZs에 리소스를 배포하는 것은 아키텍처 내에서 고가용성을 보장하는 AWS 모범 사례입니다. 가용성은 기밀성, 무결성, 가용성 3중 보안 모델의 핵심 요소입니다. VPC에 연결하는 모든 Lambda 함수는 단일 장애 영역으로 인해 운영이 완전히 중단되지 않도록 다중 AZ 배포를 포함해야 합니다.

문제 해결

계정의 VPC에 연결하도록 함수를 구성하는 경우, 고가용성을 보장하기 위해 여러 AZ에 서브넷을 지정합니다. 지침은 AWS Lambda 개발자 안내서의 VPC 액세스 구성을 참조하세요.

Lambda는 단일 영역에서 서비스 중단이 발생할 경우, 이벤트를 처리할 수 있도록 여러 AZ에서 다른 함수를 자동으로 실행합니다.

[Lambda.6] Lambda 함수에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: `tagged-lambda-function` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| requiredTagKeys | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | No default value |

이 제어는 AWS Lambda 함수에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다requiredTagKeys. 함수에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 함수에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 를 AWS 서비스포함하여 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태깅 모범 사례에 대한 자세한 내용은 AWS 일반 참조의 AWS 리소스 태깅을 참조하세요.

문제 해결

Lambda 함수에 태그를 추가하려면 AWS Lambda 개발자 안내서의 Lambda 함수에서 태그 사용을 참조하세요.

[Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::Lambda::Function`

AWS Config 규칙: lambda-function-xray-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Lambda 를 사용한 활성 추적 AWS X-Ray 이 함수에 대해 활성화되어 있는지 확인합니다. Lambda 함수에 대해 X-Ray를 사용한 활성 추적이 비활성화된 경우 제어가 실패합니다.

AWS X-Ray 는 AWS Lambda 함수에 대한 추적 및 모니터링 기능을 제공하여 Lambda 함수를 디버깅하고 운영하는 데 드는 시간과 노력을 절약할 수 있습니다. 이 서비스는 Lambda 함수의 지연 시간을 분석하여 오류를 진단하고 성능 병목 현상, 속도 저하, 시간 초과를 식별하는 데 도움이 될 수 있습니다. 또한 데이터 프라이버시 및 규정 준수 요구 사항에도 유용할 수 있습니다. Lambda 함수에 대해 활성 추적을 활성화하면 X-Ray가 Lambda 함수 내의 데이터 흐름 및 처리에 대한 전체적인 보기를 제공하므로 잠재적 보안 취약성 또는 규정 미준수 데이터 처리 사례를 식별하는 데 도움이 될 수 있습니다. 이러한 가시성을 통해 데이터 무결성, 기밀성 및 관련 규정 준수를 유지할 수 있습니다.

> **Note**
>
> AWS X-Ray 추적은 현재 Amazon Managed Streaming for Apache Kafka(Amazon MSK), 자체 관리형 Apache Kafka, ActiveMQ 및 RabbitMQ를 사용하는 Amazon MQ 또는 Amazon DocumentDB 이벤트 소스 매핑을 사용하는 Lambda 함수에는 지원되지 않습니다. RabbitMQ

문제 해결

AWS Lambda 함수에 대한 활성 추적 활성화에 대한 자세한 내용은 AWS Lambda 개발자 안내서의를 사용하여 Lambda 함수 호출 시각화 AWS X-Ray를 참조하세요.

## Macie에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Macie 서비스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Macie.1] Amazon Macie가 활성화되어야 합니다.

관련 요구 사항: 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

범주: 감지 > 감지 서비스

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: `macie-status-check`

스케줄 유형: 주기적

이 제어는 계정에 Amazon Macie가 활성화되어 있는지 확인합니다. 계정에 Macie가 활성화되어 있지 않으면 제어가 실패합니다.

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 민감한 데이터를 검색하고, 데이터 보안 위험에 대한 가시성을 제공하며, 이러한 위험에 대한 자동 보호를 지원합니다. Macie는 Amazon Simple Storage Service(S3) 버킷의 보안 및 액세스 제어를 자동으로 지속적으로 평가하고, 조사 결과를 생성하여 Amazon S3 데이터의 보안 또는 프라이버시와 관련된 잠재적인 문제를 알려줍니다. 또한 Macie는 개인 식별 정보(PII)와 같은 민감한 데이터의 검색 및 보고를 자동화하여 Amazon S3에 저장하는 데이터를 더 잘 이해할 수 있도록 합니다. 자세한 내용은 Amazon Macie 사용 설명서를 참조하세요.

문제 해결

Macie를 활성화하려면 Amazon Macie 사용 설명서의 Macie 활성화를 참조하세요.

[Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.

관련 요구 사항: 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

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::::Account`

AWS Config 규칙: `macie-auto-sensitive-data-discovery-check`

스케줄 유형: 주기적

이 제어는 Amazon Macie 관리자 계정에 민감한 데이터 자동 검색이 활성화되어 있는지 확인합니다. Macie 관리자 계정에 민감한 데이터 자동 검색을 활성화하지 않으면 제어가 실패합니다. 이 제어는 관리자 계정에만 적용됩니다.

Macie는 Amazon Simple Storage Service(Amazon S3) 버킷에서 개인 식별 정보(PII)와 같은 민감한 데이터의 검색 및 보고를 자동화합니다. Macie는 민감한 데이터 자동 검색을 통해 버킷 인벤토리를 지속적으로 평가하고 샘플링 기법을 사용하여 버킷의 대표적인 S3 객체를 식별하고 선택합니다. 그런 다음 Macie는 선택한 객체를 검색 및 분석하여 민감한 데이터가 있는지 검사합니다. 분석이 진행됨에 따라 Macie는 Amazon S3 데이터에 대해 제공하는 통계, 인벤토리 데이터 및 기타 정보를 업데이트합니다. Macie는 또한 발견한 민감한 데이터를 보고하는 조사 결과를 생성합니다.

문제 해결

S3 버킷의 객체를 분석하기 위한 민감한 데이터 자동 검색 작업을 생성하고 구성하려면 Amazon Macie 사용 설명서의 계정에 대한 민감한 데이터 자동 검색 구성을 참조하세요.

## Amazon MSK에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::MSK::Cluster`

AWS Config 규칙: msk-in-cluster-node-require-tls

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK 클러스터가 클러스터의 브로커 노드 사이에서 HTTPS(TLS)를 사용하여 전송 중 암호화되었는지 확인합니다. 클러스터 브로커 노드 연결에 일반 텍스트 통신이 활성화된 경우, 제어가 실패합니다.

HTTPS는 TLS를 사용하여 데이터를 이동하므로 추가 보안 계층을 제공하며 잠재적 공격자가 중간자 또는 그와 유사한 공격을 사용하여 네트워크 트래픽을 염탐하거나 조작하지 못하게 하는 데 사용할 수 있습니다. 기본적으로 Amazon MSK는 TLS를 사용하여 전송 중 데이터를 암호화합니다. 그러나 클러스터를 생성할 때 이 기본값을 재정의할 수 있습니다. 브로커 노드 연결에는 HTTPS(TLS)를 통한 암호화된 연결을 사용하는 것이 좋습니다.

문제 해결

Amazon MSK 클러스터의 암호화 설정을 업데이트하는 방법에 대한 자세한 내용은 Amazon Managed Streaming for Apache Kafka 개발자 안내서의 클러스터 보안 설정 업데이트를 참조하세요.

[MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::MSK::Cluster`

AWS Config 규칙: msk-enhanced-monitoring-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK 클러스터에 `PER_TOPIC_PER_BROKER` 이상의 모니터링 수준으로 지정된 향상된 모니터링이 구성되어 있는지 확인합니다. 클러스터의 모니터링 수준이 `DEFAULT` 또는 `PER_BROKER`로 설정된 경우, 제어가 실패합니다.

`PER_TOPIC_PER_BROKER` 모니터링 수준은 MSK 클러스터의 성능에 대한 보다 세밀한 인사이트를 제공하고 CPU 및 메모리 사용량 등 리소스 사용률과 관련된 메트릭도 제공합니다. 이를 통해 개별 주제 및 브로커의 성능 병목 현상과 리소스 사용 패턴을 식별할 수 있습니다. 이러한 가시성을 통해 결국 Kafka 브로커의 성능을 최적화할 수 있습니다.

문제 해결

MSK 클러스터에 대한 향상된 모니터링을 구성하려면 다음 단계를 완료하세요.

1. https://console.aws.amazon.com/msk/home?region=us-east-1#/home/에서 Amazon MSK 콘솔을 엽니다.
2. 탐색 창에서 클러스터를 선택합니다. 그런 다음 클러스터를 선택합니다.
3. 작업에서 모니터링 편집을 선택합니다.
4. 향상된 주제 수준 모니터링 옵션을 선택합니다.
5. 변경 사항 저장을 선택합니다.

모니터링 수준에 대한 자세한 내용은 Amazon Managed Streaming for Apache Kafka 개발자 안내서의 CloudWatch를 사용하여 표준 브로커를 모니터링하기 위한 Amazon MSK 지표를 참조하세요.

[MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.

관련 요구 사항: PCI DSS v4.0.1/4.2.1

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::KafkaConnect::Connector`

AWS Config규칙: `msk-connect-connector-encrypted` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK Connect 커넥터가 전송 중에 암호화되었는지 확인합니다. 전송 중에 커넥터가 암호화되지 않으면 이 제어가 실패합니다.

전송 중 데이터는 클러스터의 노드 사이 또는 클러스터와 애플리케이션 사이와 같이 한 위치에서 다른 위치로 이동하는 데이터를 나타냅니다. 데이터는 인터넷 또는 프라이빗 네트워크 내에서 이동할 수 있습니다. 전송 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다.

문제 해결

MSK Connect 커넥터를 생성할 때 전송 중 암호화를 활성화할 수 있습니다. 클러스터를 생성한 후에는 암호화 설정을 변경할 수 없습니다. 자세한 내용은 Amazon Managed Streaming for Apache Kafka 개발자 안내서의 커넥터 생성을 참조하세요.

[MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::MSK::Cluster`

AWS Config 규칙: msk-cluster-public-access-disabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK 클러스터에 퍼블릭 액세스가 비활성화되어 있는지 확인합니다. MSK 클러스터에 대해 퍼블릭 액세스가 활성화된 경우 제어가 실패합니다.

기본적으로 클라이언트는 Amazon MSK 클러스터와 동일한 VPC에 있는 경우에만 클러스터에 액세스할 수 있습니다. Kafka 클라이언트와 MSK 클러스터 간의 모든 통신은 기본적으로 프라이빗이며 스트리밍 데이터는 인터넷을 통과하지 않습니다. 그러나 MSK 클러스터가 퍼블릭 액세스를 허용하도록 구성된 경우 인터넷 상의 모든 사용자가 해당 클러스터 내에서 실행 중인 Apache Kafka 브로커에 대한 연결을 설정할 수 있습니다. 이로 인해 무단 액세스, 데이터 침해, 취약성 악용과 같은 문제가 발생할 수 있습니다. 인증 및 권한 부여 조치를 요구하여 클러스터에 대한 액세스를 제한하면 민감한 정보를 보호하고 리소스의 무결성을 유지하는 데 도움이 될 수 있습니다.

문제 해결

Amazon MSK 클러스터에 대한 퍼블릭 액세스를 관리하는 방법에 대한 자세한 내용은 Amazon Managed Streaming for Apache Kafka 개발자 안내서의 MSK 프로비저닝된 클러스터에 대한 퍼블릭 액세스 활성화를 참조하세요.

[MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::KafkaConnect::Connector`

AWS Config 규칙: msk-connect-connector-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK 커넥터에 로깅이 활성화되어 있는지 확인합니다. MSK 커넥터에 대해 로깅이 비활성화된 경우 제어가 실패합니다.

Amazon MSK 커넥터는 데이터 소스의 스트리밍 데이터를 Apache Kafka 클러스터로 지속적으로 복사하거나 클러스터의 데이터를 데이터 싱크로 지속적으로 복사하여 외부 시스템 및 Amazon 서비스를 Apache Kafka와 통합합니다. MSK Connect는 커넥터 디버깅에 도움이 되는 로그 이벤트를 작성할 수 있습니다. 커넥터를 생성할 때 다음 로그 대상을 0개 이상 지정할 수 있습니다. Amazon CloudWatch Logs, Amazon S3, Amazon Data Firehose.

> **Note**
>
> 플러그인이 해당 값을 보안 암호로 정의하지 않은 경우 커넥터 로그에 민감한 구성 값이 표시될 수 있습니다. Kafka Connect는 정의되지 않은 구성 값을 기타 일반 텍스트 값과 동일하게 취급합니다.

문제 해결

기존 Amazon MSK 커넥터에 대해 로깅을 활성화하려면 적절한 로깅 구성으로 커넥터를 다시 생성해야 합니다. 구성 옵션에 대한 자세한 내용은 Amazon Managed Streaming for Apache Kafka 개발자 안내서의 MSK Connect 로깅을 참조하세요.

[MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::MSK::Cluster`

AWS Config 규칙: msk-unrestricted-access-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MSK 클러스터에 인증되지 않은 액세스가 활성화되어 있는지 확인합니다. MSK 클러스터에 대해 인증되지 않은 액세스가 활성화된 경우 제어가 실패합니다.

Amazon MSK는 클러스터에 대한 액세스를 제어하는 클라이언트 인증 및 권한 부여 메커니즘을 지원합니다. 이러한 메커니즘은 클러스터에 연결하는 클라이언트의 ID를 확인하고 클라이언트가 수행할 수 있는 작업을 결정합니다. 인증되지 않은 액세스를 허용하도록 MSK 클러스터를 구성할 수 있습니다. 이렇게 하면 네트워크 연결이 가능한 모든 클라이언트가 자격 증명을 제공하지 않고도 Kafka 주제를 게시하고 구독할 수 있습니다. 인증 요구 사항 없이 MSK 클러스터를 실행하면 최소 권한 원칙을 위반하는 것이며 클러스터가 무단 액세스에 노출될 수 있습니다. 모든 클라이언트가 Kafka 주제의 데이터를 액세스, 수정, 삭제할 수 있으므로 데이터 침해, 무단 데이터 수정 또는 서비스 중단이 발생할 수 있습니다. 적절한 액세스 제어를 보장하고 보안 규정 준수를 유지하려면 IAM 인증, SASL/SCRAM, 상호 TLS와 같은 인증 메커니즘을 활성화하는 것이 좋습니다.

문제 해결

Amazon MSK 클러스터의 인증 설정을 변경하는 방법에 대한 자세한 내용은 Amazon Managed Streaming for Apache Kafka 개발자 안내서의 Amazon MSK 클러스터의 보안 설정 업데이트 및 Apache Kafka API에 대한 인증 및 권한 부여를 참조하세요.

## Amazon MQ에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon MQ 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `mq-cloudwatch-audit-log-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MQ ActiveMQ 브로커가 감사 로그를 Amazon CloudWatch Logs로 스트리밍하는지 여부를 확인합니다. 브로커가 CloudWatch Logs에 감사 로그를 스트리밍하지 않으면 제어가 실패합니다.

ActiveMQ 브로커 로그를 CloudWatch Logs에 게시하여 보안 관련 정보의 가시성을 높이는 CloudWatch 경보 및 메트릭를 생성할 수 있습니다.

문제 해결

ActiveMQ 브로커 로그를 CloudWatch Logs로 스트리밍하려면 Amazon MQ 개발자 안내서의 ActiveMQ 로그에 대한 Amazon MQ 구성을 참조하세요.

[MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config규칙: `tagged-amazonmq-broker` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon MQ 브로커에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 브로커에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 브로커에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는

데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Amazon MQ 브로커에 태그를 추가하려면 Amazon MQ 개발자 안내서의 리소스 태깅을 참조하세요.

[MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 낮음

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `mq-active-deployment-mode`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MQ ActiveMQ 브로커의 배포 모드가 활성/대기로 설정되어 있는지 확인합니다. 단일 인스턴스 브로커(기본적으로 활성화됨)를 배포 모드로 설정하면 제어가 실패합니다.

활성/대기 배포는 AWS 리전에서 Amazon MQ ActiveMQ 브로커에 대한 고가용성을 제공합니다. 활성/대기 배포 모드에는 중복 쌍으로 구성된 두 개의 서로 다른 가용 영역에 있는 두 개의 브로커 인스턴스가 포함됩니다. 이러한 브로커는 애플리케이션과 동기적으로 통신하므로 장애 발생 시 가동 중지 시간과 데이터 손실을 줄일 수 있습니다.

문제 해결

활성/대기 배포 모드로 새로운 ActiveMQ 브로커를 생성하려면 Amazon MQ 개발자 안내서의 ActiveMQ 브로커 생성 및 구성을 참조하세요. 배포 모드에서 활성/대기 브로커를 선택합니다. 기존 브로커의 배포 모드는 변경할 수 없습니다. 대신 새로운 브로커를 생성하고 이전 브로커의 설정을 복사해야 합니다.

[MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다

관련 요구 사항: 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

범주: 복구 > 복원력 > 고가용성

심각도: 낮음

리소스 유형: `AWS::AmazonMQ::Broker`

AWS Config 규칙: `mq-rabbit-deployment-mode`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon MQ RabbitMQ 브로커의 배포 모드가 클러스터 배포로 설정되었는지 여부를 확인합니다. 단일 인스턴스 브로커(기본적으로 활성화됨)를 배포 모드로 설정하면 제어가 실패합니다.

클러스터 배포는 AWS 리전에서 Amazon MQ RabbitMQ 브로커에 대한 고가용성을 제공합니다. 클러스터 배포는 각각 자체 Amazon Elastic Block Store(Amazon EBS) 볼륨과 공유 상태를 갖는 세 개의 RabbitMQ 브로커 노드로 구성된 논리적 그룹입니다. 클러스터 배포를 통해 데이터가 클러스터의 모든 노드에 복제되므로 장애 발생 시 가동 중지 시간과 데이터 손실을 줄일 수 있습니다.

문제 해결

클러스터 배포 모드를 사용하여 새로운 RabbitMQ 브로커를 생성하려면 Amazon MQ 개발자 안내서의 RabbitMQ 브로커 생성 및 연결을 참조하세요. 배포 모드에서는 클러스터 배포를 선택합니다. 기존 브로커의 배포 모드는 변경할 수 없습니다. 대신 새로운 브로커를 생성하고 이전 브로커의 설정을 복사해야 합니다.

## Neptune에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Neptune 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터가 저장 시 암호화되어 있는지 여부를 확인합니다. Neptune DB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 해당 데이터의 기밀성을 보호하여 권한 없는 사용자가 해당 데이터에 액세스할 수 있는 위험을 줄일 수 있습니다. Neptune DB 클러스터를 암호화하면 데이터와 메타데이터를 무단 액세스로부터 보호할 수 있습니다. 또한 프로덕션 파일 시스템의 미사용 데이터 암호화에 대한 규정 준수 요구 사항도 충족합니다.

문제 해결

Neptune DB 클러스터를 만들 때 저장 시 암호화를 활성화할 수 있습니다. 클러스터를 생성한 후에는 암호화 설정을 변경할 수 없습니다. 자세한 내용은 Neptune 사용 설명서의 저장 중 Neptune 리소스 암호화를 참조하세요.

[Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-cloudwatch-log-export-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어 기능은 Neptune DB 클러스터가 Amazon CloudWatch Logs에 감사 로그를 게시하는지 여부를 확인합니다. Neptune DB 클러스터가 감사 로그를 CloudWatch Logs에 게시하지 않으면 제어가 실패합니다. `EnableCloudwatchLogsExport`은 `Audit`로 설정해야 합니다.

Amazon Neptune과 Amazon CloudWatch가 통합되어 성능 메트릭를 수집하고 분석할 수 있습니다. Neptune은 메트릭를 CloudWatch에 자동으로 전송하고 CloudWatch 경보도 지원합니다. 감사 로그는 고도로 사용자 지정이 가능합니다. 데이터베이스를 감사할 때 어떤 데이터베이스 클러스터에 액세스하고 어떻게 액세스하는지에 대한 정보를 포함하여 데이터에 대한 각 작업을 모니터링하고 감사 추적에 기록할 수 있습니다. Neptune DB 클러스터를 모니터링하는 데 도움이 되도록 이러한 로그를 CloudWatch로 보내는 것이 좋습니다.

문제 해결

Neptune 감사 로그를 CloudWatch Logs에 게시하려면 Neptune 사용 설명서의 Amazon CloudWatch Logs에 Neptune 로그 게시를 참조하세요. 로그 내보내기 섹션에서 감사를 선택합니다.

[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::RDS::DBClusterSnapshot`

AWS Config 규칙: `neptune-cluster-snapshot-public-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune 수동 DB 클러스터 스냅샷이 퍼블릭인지 여부를 확인합니다. Neptune 수동 DB 클러스터 스냅샷이 퍼블릭인 경우, 제어가 실패합니다.

Neptune DB 클러스터 수동 스냅샷은 의도하지 않는 한 공개해서는 안 됩니다. 암호화되지 않은 수동 스냅샷을 공개로 공유하면 모든 AWS 계정에서 해당 스냅샷을 사용할 수 있습니다. 퍼블릭 스냅샷은 의도하지 않은 데이터 노출을 초래할 수 있습니다.

문제 해결

Neptune 수동 DB 클러스터 스냅샷에 대한 퍼블릭 액세스를 제거하려면 Neptune 사용 설명서의 DB 클러스터 스냅샷 공유를 참조하세요.

[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터의 삭제 방지 기능 활성화 여부를 확인합니다. Neptune DB 클러스터에 삭제 방지 기능이 활성화되지 않은 경우, 제어가 실패합니다.

클러스터 삭제 방지를 활성화하면 우발적인 데이터베이스 삭제 또는 권한 없는 사용자에 의한 삭제에 대한 추가 보호 계층이 제공됩니다. 삭제 방지가 활성화된 동안에는 Neptune DB 클러스터를 삭제할 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 방지를 비활성화해야 합니다.

문제 해결

기존 Neptune DB 클러스터에 대한 삭제 방지를 활성화하려면 Amazon Aurora 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하세요.

[Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 SI-12

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-backup-retention-check`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `minimumBackupRetentionPeriod` | 백업 보존 기간(일수) | Integer | 7~35 | 7 | |

이 제어는 Neptune DB 클러스터에 자동 백업이 활성화되어 있고 백업 보존 기간이 지정된 기간 이상인지 확인합니다. Neptune DB 클러스터에 대한 백업이 활성화되지 않았거나 보존 기간이 지정된 기간 미만인 경우, 제어가 실패합니다. 백업 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구하고 시스템의 복원력을 강화할 수 있습니다. Neptune DB 클러스터의 백업을 자동화하면 시스템을 특정 시점으로 복원하고 가동 중지 시간과 데이터 손실을 최소화할 수 있습니다.

문제 해결

자동 백업을 활성화하고 Neptune DB 클러스터의 백업 보존 기간을 설정하려면 Amazon RDS 사용 설명서의 자동 백업 활성화를 참조하세요. 백업 보존 기간의 경우, 7 이상의 값을 선택합니다.

[Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBClusterSnapshot`

AWS Config 규칙: `neptune-cluster-snapshot-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터 스냅샷이 저장 시 암호화되었는지 여부를 확인합니다. Neptune DB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 이러한 데이터의 기밀을 보호하여 권한이 없는 사용자가 데이터에 액세스할 위험을 줄일 수 있습니다. Neptune DB 클러스터 스냅샷의 데이터는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다.

문제 해결

기존 Neptune DB 클러스터 스냅샷은 암호화할 수 없습니다. 대신 스냅샷을 새로운 DB 클러스터에 복원하고 클러스터에서 암호화를 활성화해야 합니다. 암호화된 클러스터에서 암호화된 스냅샷을 생성할 수 있습니다. 지침은 Neptune 사용 설명서의 DB 클러스터 스냅샷에서 복원 및 Neptune에서 DB 클러스터 스냅샷 생성을 참조하세요.

[Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-iam-database-authentication`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Neptune DB 클러스터에 IAM 데이터베이스 인증이 활성화되어 있는지 확인합니다. Neptune DB 클러스터에 대해 IAM 데이터베이스 인증이 활성화되지 않은 경우, 제어가 실패합니다.

Amazon Neptune 데이터베이스 클러스터에 대한 IAM 데이터베이스 인증을 사용하면 인증을 IAM을 사용해 외부에서 관리하기 때문에 데이터베이스 구성 내에 사용자 보안 인증을 저장할 필요가 없습니다. IAM 데이터베이스 인증이 활성화된 경우 각 요청은 AWS서명 버전 4를 사용하여 서명해야 합니다.

문제 해결

기본적으로 Neptune DB 클러스터를 생성하면 IAM 데이터베이스 인증이 비활성화됩니다. 이를 활성화하려면 Neptune 사용 설명서의 Neptune에서 IAM 데이터베이스 인증 활성화를 참조하세요.

[Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-copy-tags-to-snapshot-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 스냅샷이 생성될 때 Neptune DB 클러스터가 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다. Neptune DB 클러스터가 태그를 스냅샷에 복사하도록 구성되지 않은 경우, 제어가 실패합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 상위 Amazon RDS 데이터베이스 클러스터와 동일한 방식으로 스냅샷에 태그를 지정해야 합니다. 태그를 복사하면 DB 스냅샷의 메타데이터가 상위 데이터베이스 클러스터의 메타데이터와 일치하고, DB 스냅샷의 액세스 정책도 상위 DB 인스턴스의 액세스 정책과 일치하게 됩니다.

문제 해결

Neptune DB 클러스터의 스냅샷에 태그를 복사하려면 Neptune 사용 설명서의 Neptune에서 태그 복사를 참조하세요.

[Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `neptune-cluster-multi-az-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Neptune DB 클러스터의 여러 가용 영역(AZ)에 읽기 전용 복제본 인스턴스가 있는지 확인합니다. 클러스터를 하나의 AZ에만 배포하면 제어가 실패합니다.

AZ를 사용할 수 없고 정기적인 유지 관리 이벤트가 발생하는 경우, 읽기 전용 복제본은 기본 인스턴스의 장애 조치 대상 역할을 합니다. 즉, 기본 인스턴스에 장애가 발생하면 Neptune은 읽기 전용 복제본 인스턴스를 기본 인스턴스로 승격합니다. 반대로 DB 클러스터에 읽기 전용 복제본 인스턴스가 포함되어 있지 않으면 기본 인스턴스에 장애가 발생해도 DB 클러스터를 다시 만들 때까지 사용할 수 없습니다. 기본 인스턴스를 다시 만드는 것은 읽기 전용 복제본을 승격하는 것보다 훨씬 더 오래 걸립니다. 고가용성을 보장하려면 기본 인스턴스와 동일한 DB 인스턴스 클래스를 갖고 기본 인스턴스와는 다른 AZ에 위치한 하나 이상의 읽기 전용 복제본 인스턴스를 생성하는 것이 좋습니다.

문제 해결

여러 AZ에 Neptune DB 클러스터를 배포하려면 Neptune 사용 설명서의 Neptune DB 클러스터의 읽기 전용 복제본 DB 인스턴스를 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Network Firewall

이러한 AWS Security Hub CSPM제어는 AWS Network Firewall서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::Firewall`

AWS Config 규칙: netfw-multi-az-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는를 통해 관리되는 방화벽AWS Network Firewall이 여러 가용 영역(AZs)에 배포되는지 여부를 평가합니다. 방화벽을 하나의 AZ에만 배포하면 제어가 실패합니다.

AWS글로벌 인프라에는 여러가 포함됩니다AWS 리전. AZ는 각 리전 내에서 물리적으로 분리되고 격리된 위치로, 이러한 위치는 짧은 지연 시간, 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 여러 AZ에 Network Firewall 방화벽을 배포하면 AZ 간에 트래픽을 분산하고 이동할 수 있으므로 고가용성 솔루션을 설계하는 데 도움이 됩니다.

문제 해결

여러 AZ에 Network Firewall 방화벽 배포

1. https://console.aws.amazon.com/vpc/에서 Amazon VPC 콘솔을 엽니다.

2. 탐색 창의 Network Firewall에서 방화벽을 선택합니다.
3. 방화벽 페이지에서 편집하려는 방화벽을 선택합니다.
4. 방화벽 세부 정보 페이지에서 방화벽 세부 정보 탭을 선택합니다.
5. 관련 정책 및 VPC 섹션에서 편집을 선택합니다.
6. 새로운 AZ를 추가하려면 새로운 서브넷 추가를 선택합니다. 사용할 AZ와 서브넷을 선택합니다. 두 개 이상의 AZ를 선택해야 합니다.
7. 저장을 선택합니다.

[NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.

관련 요구 사항: 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), NIST.800-171.r2 3.1.20, NIST.800-171.r2 3.13.1

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::LoggingConfiguration`

AWS Config 규칙: netfw-logging-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS Network Firewall방화벽에 로깅이 활성화되어 있는지 확인합니다. 하나 이상의 로그 유형에 대해 로깅이 활성화되지 않았거나 로깅 대상이 존재하지 않는 경우, 제어가 실패합니다.

로깅은 방화벽의 안정성, 가용성 및 성능을 유지하는 데 도움이 됩니다. Network Firewall에서 로깅은 상태 저장 엔진이 패킷 흐름을 받은 시간, 패킷 흐름에 대한 상세 정보, 패킷 흐름에 대해 수행된 상태 저장 규칙 동작을 비롯해 네트워크 트래픽에 대한 자세한 정보를 제공합니다.

문제 해결

방화벽 로깅을 활성화하려면 AWS Network Firewall 개발자 안내서의 방화벽 로깅 구성 업데이트를 참조하세요.

[NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.13.1

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config 규칙: netfw-policy-rule-group-associated

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 네트워크 방화벽 정책에 상태 저장 또는 상태 비저장 규칙 그룹이 연결되어 있는지 확인합니다. 상태 비저장 또는 상태 저장 규칙 그룹이 할당되지 않으면 제어가 실패합니다.

방화벽 정책은 Amazon Virtual Private Cloud(Amazon VPC)에서 방화벽이 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하면 패킷과 트래픽 흐름을 필터링하는 데 도움이 되며 기본 트래픽 처리를 정의합니다.

문제 해결

네트워크 방화벽 정책에 규칙 그룹을 추가하려면 AWS Network Firewall 개발자 가이드에서 방화벽 정책 업데이트를 참조하세요. 규칙 그룹을 만들고 관리하는 방법에 대한 자세한 내용은 AWS Network Firewall의 규칙 그룹을 참조하세요.

[NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config 규칙: netfw-policy-default-action-full-packets

스케줄 유형: 변경이 트리거됨

파라미터:

- `statelessDefaultActions: aws:drop,aws:forward_to_sfe`(사용자 지정할 수 없음)

이 제어는 네트워크 방화벽 정책의 전체 패킷에 대한 기본 상태 비저장 작업이 삭제인지 전달인지 확인합니다. `Drop` 또는 `Forward`를 선택하면 제어가 통과하고, `Pass`를 선택하면 제어가 실패합니다.

방화벽 정책은 방화벽이 Amazon VPC의 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링합니다. `Pass`를 기본값으로 설정하면 의도하지 않은 트래픽이 허용될 수 있습니다.

문제 해결

방화벽 정책을 변경하려면 AWS Network Firewall 개발자 안내서의 방화벽 정책 업데이트를 참조하세요. 상태 비저장 기본 작업에서 편집을 선택합니다. 그런 다음 작업으로 삭제 또는 상태 저장 규칙 그룹으로 전달을 선택합니다.

[NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.6

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config 규칙: netfw-policy-default-action-fragment-packets

스케줄 유형: 변경이 트리거됨

파라미터:

- `statelessFragDefaultActions (Required) : aws:drop, aws:forward_to_sfe`(사용자 지정할 수 없음)

이 제어는 네트워크 방화벽 정책의 조각화된 패킷에 대한 기본 상태 비저장 작업이 삭제인지 전달인지 확인합니다. `Drop` 또는 `Forward`를 선택하면 제어가 통과하고, `Pass`를 선택하면 제어가 실패합니다.

방화벽 정책은 방화벽이 Amazon VPC의 트래픽을 모니터링하고 처리하는 방법을 정의합니다. 상태 비저장 및 상태 저장 규칙 그룹을 구성하여 패킷과 트래픽 흐름을 필터링합니다. `Pass`를 기본값으로 설정하면 의도하지 않은 트래픽이 허용될 수 있습니다.

문제 해결

방화벽 정책을 변경하려면 AWS Network Firewall 개발자 안내서의 방화벽 정책 업데이트를 참조하세요. 상태 비저장 기본 작업에서 편집을 선택합니다. 그런 다음 작업으로 삭제 또는 상태 저장 규칙 그룹으로 전달을 선택합니다.

[NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.

관련 요구 사항: 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(5), NIST.800-171.r2 3.1.3, NIST.800-171.r2 3.1.14, NIST.800-171.r2 3.13.1, NIST.800-171.r2 3.13.6

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::RuleGroup`

AWS Config 규칙: netfw-stateless-rule-group-not-empty

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는의 상태 비저장 규칙 그룹에 규칙이 AWS Network Firewall포함되어 있는지 확인합니다. 규칙 그룹에 규칙이 없으면 제어가 실패합니다.

규칙 그룹에는 방화벽이 VPC의 트래픽을 처리하는 방법을 정의하는 규칙이 포함되어 있습니다. 빈 상태 비저장 규칙 그룹이 방화벽 정책에 존재하면 규칙 그룹이 트래픽을 처리할 것 같은 인상을 줄 수 있습니다. 하지만 상태 비저장 규칙 그룹이 비어 있으면 트래픽을 처리하지 않습니다.

문제 해결

Network Firewall 규칙 그룹에 규칙을 추가하려면 AWS Network Firewall 개발자 안내서의 상태 저장 규칙 그룹 업데이트를 참조하세요. 방화벽 세부 정보 페이지에서 상태 비저장 규칙 그룹에 대해 편집을 선택하여 규칙을 추가합니다.

[NetworkFirewall.7] 네트워크 방화벽에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::NetworkFirewall::Firewall`

AWS Config규칙: `tagged-networkfirewall-firewall` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS Network Firewall방화벽에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 방화벽에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 방화벽에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Network Firewall 방화벽에 태그를 추가하려면 AWS Network Firewall개발자 안내서의 AWS Network Firewall리소스 태그 지정을 참조하세요.

[NetworkFirewall.8] 네트워크 방화벽 정책에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config규칙: `tagged-networkfirewall-firewallpolicy` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS Network Firewall방화벽 정책에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 방화벽 정책에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 방화벽 정책에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수

있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Network Firewall 정책에 태그를 추가하려면 AWS Network Firewall개발자 안내서의 AWS Network Firewall리소스 태그 지정을 참조하세요.

[NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::Firewall`

AWS Config 규칙: netfw-deletion-protection-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Network Firewall방화벽에 삭제 방지 기능이 활성화되어 있는지 확인합니다. 방화벽에 삭제 방지가 활성화되어 있지 않으면 제어가 실패합니다.

AWS Network Firewall는 Virtual Private Cloud(VPCs. 삭제 방지 설정은 실수로 방화벽을 삭제하는 것을 방지합니다.

문제 해결

기존 Network Firewall 방화벽에서 삭제 방지를 활성화하려면 AWS Network Firewall 개발자 안내서의 방화벽 업데이트를 참조하세요. 변경 방지에 대해서는 활성화를 선택합니다.

UpdateFirewallDeleteProtection API를 호출하고 `DeleteProtection` 필드를 `true`로 설정하여 삭제 방지를 활성화할 수도 있습니다.

[NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다

관련 요구 사항: 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)

범주: 보호 > 네트워크 보안

심각도: 중간

리소스 유형: `AWS::NetworkFirewall::Firewall`

AWS Config 규칙: netfw-subnet-change-protection-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Network Firewall 방화벽에 서브넷 변경 방지가 활성화되어 있는지 확인합니다. 방화벽에 서브넷 변경 방지가 활성화되어 있지 않으면 제어가 실패합니다.

AWS Network Firewall는 Virtual Private Cloud(VPCs. Network Firewall 방화벽에 대해 서브넷 변경 방지를 활성화하면 방화벽의 서브넷 연결이 실수로 변경되는 것을 방지하여 방화벽을 보호할 수 있습니다.

문제 해결

기존 Network Firewall 방화벽에서 서브넷 변경 방지를 활성화하는 방법에 대한 자세한 내용은 AWS Network Firewall 개발자 안내서의 방화벽 업데이트를 참조하세요.

## Amazon OpenSearch Service에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon OpenSearch Service(OpenSearch Service) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-encrypted-at-rest`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 OpenSearch 도메인에 저장 시 암호화 구성이 활성화되어 있는지 확인합니다. 유휴 시 암호화가 활성화되지 않은 경우, 이 확인이 실패합니다.

민감한 데이터에 대한 보안 계층을 추가하려면 OpenSearch Service 도메인이 저장 시 암호화되도록 구성해야 합니다. 저장 데이터 암호화를 구성하면가 암호화 키를 AWS KMS저장하고 관리합니다. 암호화를 수행하려면 256비트 키(AES-256)가 있는 고급 암호화 표준 알고리즘을 AWS KMS사용합니다.

OpenSearch Service 저장 시 암호화에 대해 자세히 알아보려면 Amazon OpenSearch Service 개발자 안내서의 Amazon OpenSearch Service에 대한 저장 데이터 암호화를 참조하세요.

문제 해결

새로운 및 기존 OpenSearch 도메인에 대해 저장 시 암호화를 활성화려면 Amazon OpenSearch Service 개발자 안내서의 저장 데이터 암호화 활성화를 참조하세요.

[Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 심각

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-in-vpc-only`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 OpenSearch 도메인이 VPC에 있는지 확인합니다. 퍼블릭 액세스를 확인하기 위해 VPC 서브넷 라우팅 구성을 평가하지 않습니다.

OpenSearch 도메인이 퍼블릭 서브넷에 연결되어 있지 않은지 확인해야 합니다. Amazon OpenSearch Service 개발자 안내서의 리소스 기반 정책을 참조하세요. 또한 권장 모범 사례에 따라 VPC가 구성되었는지 확인해야 합니다. 또한 Amazon VPC 사용 설명서에서 VPC에 대한 보안 모범 사례를 참조하세요.

VPC 내에 배포된 OpenSearch 도메인은 퍼블릭 인터넷을 통과할 필요 없이 프라이빗 AWS네트워크를 통해 VPC 리소스와 통신할 수 있습니다. 이 구성은 전송 중 데이터에 대한 액세스를 제한하여 보안 상태를 강화합니다. VPC는 네트워크 ACL 및 보안 그룹을 포함하여 OpenSearch 도메인에 대한 액세스를 보호하기 위한 다양한 네트워크 제어를 제공합니다. Security Hub는 퍼블릭 OpenSearch 도메인을 VPC로 마이그레이션하여 이러한 제어를 활용할 것을 권장합니다.

문제 해결

퍼블릭 엔드포인트가 있는 도메인을 만들 경우, 나중에 해당 도메인을 VPC 안에 배치할 수 없습니다. 대신에 새로운 도메인을 만들어 데이터를 마이그레이션해야 합니다. 반대의 경우도 마찬가지입니다. VPC 내에 도메인을 만들 경우, 퍼블릭 엔드포인트를 가질 수 없습니다. 대신 다른 도메인을 만들거나 이 제어를 비활성화해야 합니다.

자세한 내용을 알아보려면 Amazon OpenSearch Service 개발자 안내서의 VPC 내에서 Amazon OpenSearch Service 도메인 시작을 참조하세요.

[Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-node-to-node-encryption-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 OpenSearch 도메인에 노드 간 암호화가 활성화되어 있는지 확인합니다. 도메인에서 노드 간 암호화를 비활성화하면 이 제어가 실패합니다.

HTTPS(TLS)를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 통해 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. OpenSearch 도메인에 대해 노드 간 암호화를 활성화하면 클러스터 내 통신이 전송 중 암호화됩니다.

이 구성과 관련하여 성능이 저하될 수 있습니다. 이 옵션을 활성화하기 전에 성능 균형을 파악하고 테스트해야 합니다.

문제 해결

OpenSearch 도메인에서 노드 간 암호화 활성화에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 노드 간 암호화 활성화를 참조하세요.

[Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-logs-to-cloudwatch`

스케줄 유형: 변경이 트리거됨

파라미터:

- `logtype = 'error'`(사용자 지정할 수 없음)

이 제어는 OpenSearch 도메인이 CloudWatch Logs에 오류 로그를 전송하도록 구성되어 있는지 확인합니다. 도메인에 대해 CloudWatch에 대한 오류 로깅이 활성화되지 않은 경우, 이 제어는 실패합니다.

OpenSearch 도메인의 오류 로그를 활성화하고 해당 로그를 CloudWatch Logs로 전송하여 보존 및 응답을 받아야 합니다. 도메인 오류 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

문제 해결

로그 게시를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 로그 게시 활성화(콘솔)를 참조하세요.

[Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-audit-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

- `cloudWatchLogsLogGroupArnList` (사용자 지정할 수 없음) - Security Hub CSPM은이 파라미터를 채우지 않습니다. 감사 로그용으로 구성해야 하는 CloudWatch Logs 로그 그룹을 쉼표로 구분한 목록입니다.

이 제어는 OpenSearch 도메인에 감사 로깅이 활성화되어 있는지 여부를 확인합니다. OpenSearch 도메인에 감사 로깅이 활성화되어 있지 않으면 이 제어가 실패합니다.

감사 로그는 고도로 사용자 지정이 가능합니다. 이를 통해 인증 성공 및 실패, OpenSearch에 대한 요청, 인덱스 변경 및 들어오는 검색 쿼리를 포함하여 OpenSearch 클러스터에서 사용자 활동을 추적할 수 있습니다.

문제 해결

감사 로그 활성화에 대한 지침은 Amazon OpenSearch Service 개발자 안내서의 감사 로그 활성화를 참조하세요.

[Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-data-node-fault-tolerance`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 OpenSearch 도메인이 3개 이상의 데이터 노드로 구성되어 있고 `zoneAwarenessEnabled`이 `true`인지 확인합니다. `instanceCount`이 3보다 작거나 `zoneAwarenessEnabled`이 `false`인 경우, OpenSearch 도메인에 대한 이 제어가 실패합니다.

클러스터 수준 고가용성 및 내결함성을 달성하려면 OpenSearch 도메인에 최소 3개의 데이터 노드가 있어야 합니다. 3개 이상의 데이터 노드가 포함된 OpenSearch 도메인을 배포하면 노드에 장애가 발생하더라도 클러스터 운영이 보장됩니다.

문제 해결

OpenSearch 도메인의 데이터 노드 수를 수정하려면

1. AWS콘솔에 로그인하고 https://console.aws.amazon.com/aos/ Amazon OpenSearch Service 콘솔을 엽니다.
2. 내 도메인에서 편집할 도메인의 이름을 선택하고 편집을 선택합니다.
3. 데이터 노드에서 노드 수를 3보다 큰 수로 설정합니다. 3개의 가용 영역에 배포하는 경우, 가용 영역 간에 균등하게 분배되도록 수를 3의 배수로 설정하세요.
4. 제출을 선택합니다.

[Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 민감한 API 작업 제한

심각도: 높음

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-access-control-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 OpenSearch 도메인에 세분화된 액세스 제어가 활성화되어 있는지 확인합니다. 세분화된 액세스 제어가 비활성화된 경우, 제어에 실패합니다. 세분화된 접근 제어를 위해서는 `advanced-security-options`에서 OpenSearch 파라미터 `update-domain-config`을 활성화해야 합니다.

세분화된 액세스 제어를 사용하면 추가적인 방법으로 Amazon OpenSearch Service에서 데이터에 대한 액세스를 제어할 수 있습니다.

문제 해결

세분화된 액세스 제어를 활성화하려면 Amazon OpenSearch Service 개발자 안내서의 Amazon OpenSearch Service에서 세분화된 액세스 제어를 참조하세요.

[Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-https-required`

스케줄 유형: 변경이 트리거됨

파라미터:

- `tlsPolicies: Policy-Min-TLS-1-2-PFS-2023-10`(사용자 지정할 수 없음)

이 제어는 Amazon OpenSearch Service 도메인 엔드포인트가 최신 TLS 보안 정책을 사용하도록 구성되어 있는지 확인합니다. OpenSearch 도메인 엔드포인트가 지원되는 최신 정책을 사용하도록 구성되지 않았거나 HTTP가 활성화되지 않으면 제어가 실패합니다.

HTTPS(TLS)를 사용하여 잠재적 공격자가 중간자 또는 그와 유사한 공격을 사용하여 네트워크 트래픽을 염탐하거나 조작하지 못하게 할 수 있습니다. HTTPS(TLS)를 통한 암호화된 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다. TLS 1.2는 이전 버전의 TLS보다 몇 가지 향상된 보안 기능을 제공합니다.

문제 해결

TLS 암호화를 활성화하려면 UpdateDomainConfig API 작업을 사용하세요. DomainEndpointOptions 필드를 구성하여 `TLSSecurityPolicy`에 대한 값을 지정합니다. 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 노드 간 암호화를 참조하세요.

[Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config규칙: `tagged-opensearch-domain` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon OpenSearch Service 도메인에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 도메인에 태그 키가 없거나 파라미터 `requiredTagKeys`에 모든 키

가 지정되지 않은 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이(가) 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 도메인에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

OpenSearch Service 도메인에 태그를 추가하려면 Amazon OpenSearch Service 개발자 안내서의 태그 작업을 참조하세요.

[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-update-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon OpenSearch Service 도메인에 최신 소프트웨어 업데이트가 설치되어 있는지 확인합니다. 소프트웨어 업데이트가 제공되지만 도메인에 설치되지 않은 경우, 제어가 실패합니다.

OpenSearch Service 소프트웨어 업데이트는 환경에 사용할 수 있는 최신 플랫폼 수정, 업데이트 및 기능을 제공합니다. 패치 설치를 최신 상태로 유지하면 도메인 보안 및 가용성을 유지하는 데 도움이 됩니다. 필수 업데이트에 대해 아무 작업도 수행하지 않으면 (보통 2주 후) 서비스 소프트웨어가 자동으로 업데이트됩니다. 서비스 중단을 최소화하려면 도메인 트래픽이 적은 시간대에 업데이트를 예약하는 것이 좋습니다.

문제 해결

OpenSearch 도메인에 대한 소프트웨어 업데이트를 설치하려면 Amazon OpenSearch Service 개발자 안내서의 업데이트 시작을 참조하세요.

[Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.

관련 요구 사항: 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

범주: 복구 > 복원력 > 고가용성

심각도: 낮음

리소스 유형: `AWS::OpenSearch::Domain`

AWS Config 규칙: `opensearch-primary-node-fault-tolerance`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon OpenSearch Service 도메인이 3개 이상의 전용 프라이머리 노드로 구성되어 있는지 확인합니다. 도메인에 전용 프라이머리 노드가 3개 미만인 경우, 제어가 실패합니다.

Amazon OpenSearch Service는 전용 프라이머리 노드를 사용하여 클러스터 안정성을 증가합니다. 전용 프라이머리 노드는 클러스터 관리 작업을 수행하지만 데이터를 보유하지 않거나 데이터 업로드 요청에 응답하지 않습니다. 각 프로덕션 OpenSearch 도메인에 3개의 전용 프라이머리 노드를 추가하는 Multi-AZ with Standby를 사용하는 것이 좋습니다.

문제 해결

OpenSearch 도메인의 기본 노드 수를 변경하려면 Amazon OpenSearch Service 개발자 안내서의 Amazon OpenSearch Service 도메인 생성 및 관리를 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Private CA

이러한 AWS Security Hub CSPM제어는 AWS Private Certificate Authority(AWS Private CA) 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::ACMPCA::CertificateAuthority`

AWS Config 규칙: `acm-pca-root-ca-disabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS Private CA에 비활성화된 루트 인증 기관(CA)이 있는지 확인합니다. 루트 CA가 활성화되면 제어가 실패합니다.

를 사용하면 루트 CA와 하위 CA를 포함하는 CA 계층 구조를 생성할 AWS Private CA수 CAs. 특히 프로덕션 환경에서는 일상적인 작업에 루트 CA를 사용하는 것을 최소화해야 합니다. 루트 CA는 중간 CA에 대한 인증서를 발급하기 위한 용도로만 사용해야 합니다. 이렇게 하면 중간 CA가 최종 엔터티 인증서를 발급하는 일상적인 작업을 수행하는 동안 루트 CA를 손상 없이 저장할 수 있습니다.

문제 해결

루트 CA를 비활성화하려면 AWS Private Certificate Authority 사용 설명서의 CA 상태 업데이트를 참조하세요.

[PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::ACMPCA::CertificateAuthority`

AWS Config 규칙: `acmpca-certificate-authority-tagged`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWSPrivate CA 인증 기관에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredKeyTags`. 인증 기관에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. 파라미터 `requiredKeyTags`가 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 인증 기관에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는 AWS리소스 태그 지정 및 태그 편집기 사용 설명서의 모범 사례 및 전략을 참조하세요.

문제 해결

AWS프라이빗 CA 권한에 태그를 추가하려면 AWS Private Certificate Authority사용 설명서의 프라이빗 CA에 대한 태그 추가를 참조하세요.

## Amazon RDS에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon Relational Database Service(RDS) 및 Amazon RDS 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[RDS.1] RDS 스냅샷은 비공개여야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config 규칙: `rds-snapshots-public-prohibited`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS 스냅샷이 퍼블릭인지 여부를 확인합니다. RDS 스냅샷이 퍼블릭인 경우, 제어가 실패합니다. 이 제어는 RDS 인스턴스, Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터를 평가합니다.

RDS 스냅샷은 특정 시점에 RDS 인스턴스의 데이터를 백업하는 데 사용됩니다. RDS 인스턴스의 이전 상태를 복원하는 데 사용할 수 있습니다.

RDS 스냅샷은 의도하지 않은 경우, 공개 상태가 아니여야 합니다. 암호화되지 않은 수동 스냅샷을 공개로 공유하면 모든 AWS 계정에서 해당 스냅샷을 사용할 수 있습니다. 이로 인해 의도하지 않은 RDS 인스턴스 데이터가 노출될 수 있습니다.

퍼블릭 액세스를 허용하도록 구성을 변경하면 AWS Config 규칙이 최대 12시간 동안 변경 사항을 감지하지 못할 수 있습니다. AWS Config 규칙이 변경 사항을 감지할 때까지 구성이 규칙을 위반하더라도 검사는 통과합니다.

DB 스냅샷 공유에 대한 자세한 내용은 Amazon RDS 사용 설명서의 DB 스냅샷 공유를 참조하세요.

문제 해결

RDS 스냅샷에서 퍼블릭 액세스를 제거하려면 Amazon RDS 사용 설명서의 스냅샷 공유를 참조하세요. DB 스냅샷 가시성에서 비공개를 선택합니다.

[RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.2.3, CIS AWS 파운데이션 벤치마크 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-73.r5 SC-7(5)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-public-access-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 인스턴스 구성 항목의 `PubliclyAccessible` 필드를 평가하여 Amazon RDS 인스턴스에 퍼블릭 액세스가 가능한지 여부를 확인합니다.

RDS 인스턴스 구성의 `PubliclyAccessible` 값은 DB 인스턴스에 퍼블릭 액세스가 가능한지 여부를 나타냅니다. DB 인스턴스가 `PubliclyAccessible`로 구성된 경우, 퍼블릭 IP 주소로 확인되는 공개적으로 확인 가능한 DNS 이름을 가진 인터넷 경계 인스턴스입니다. DB 인스턴스에 퍼블릭 액세스가 불가한 경우, 프라이빗 IP 주소로 확인되는 DNS 이름을 가진 내부 인스턴스인 것입니다.

RDS 인스턴스를 공개적으로 액세스할 수 있도록 의도하지 않는 한 RDS 인스턴스를 `PubliclyAccessible` 값으로 구성하면 안 됩니다. 이렇게 하면 데이터베이스 인스턴스에 불필요한 트래픽이 발생할 수 있습니다.

문제 해결

RDS DB 인스턴스에서 퍼블릭 액세스를 제거하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하세요. 퍼블릭 액세스에서 아니오를 선택합니다.

[RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.2.1, CIS AWS 파운데이션 벤치마크 v3.0.0/2.3.1, CIS AWS 파운데이션 벤치마크 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-storage-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS DB 인스턴스에 스토리지 암호화가 활성화되어 있는지 확인합니다.

이 제어는 RDS DB 인스턴스용입니다. 하지만 Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터에 대한 조사 결과를 생성할 수도 있습니다. 이러한 조사 결과가 유용하지 않으면 숨길 수 있습니다.

RDS DB 인스턴스의 중요 데이터에 대한 보안을 강화하려면 RDS DB 인스턴스가 유휴 상태에서 암호화되도록 구성해야 합니다. 유휴 시 RDS DB 인스턴스 및 스냅샷을 암호화하려면 RDS DB 인스턴스에 대해 암호화 옵션을 활성화합니다. 유휴 시 암호화된 데이터에는 DB 인스턴스에 대한 기본 스토리지, 자동 백업, 읽기 전용 복제본 및 스냅샷이 포함됩니다.

RDS 암호화된 DB 인스턴스는 RDS DB 인스턴스를 호스팅하는 서버의 데이터를 개방형 표준 AES-256 암호화 알고리즘을 사용하여 암호화합니다. 데이터가 암호화되면 Amazon RDS는 성능에 최소한의 영향을 미치면서 투명하게 데이터 액세스 인증 및 암호 해독을 처리합니다. 암호화를 사용하도록 데이터베이스 클라이언트 애플리케이션을 수정하지 않아도 됩니다.

Amazon RDS 암호화는 현재 모든 데이터베이스 엔진과 스토리지 유형에 사용할 수 있습니다. Amazon RDS 암호화는 대부분의 DB 인스턴스 클래스에서 사용 가능합니다. Amazon RDS 암호화를

지원하지 않는 DB 인스턴스 클래스에 대해 알아보려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 암호화를 참조하세요.

문제 해결

Amazon RDS의 DB 인스턴스 암호화에 대한 자세한 내용은 Amazon RDS 사용 설명서의 Amazon RDS 리소스 암호화를 참조하세요.

[RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBClusterSnapshot`, `AWS::RDS::DBSnapshot`

AWS Config 규칙: `rds-snapshot-encrypted`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 스냅샷의 암호화 여부를 확인합니다. RDS DB 스냅샷이 암호화되지 않으면 제어가 실패합니다.

이 제어는 RDS DB 인스턴스용입니다. 하지만 Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터의 스냅샷에 대한 조사 결과를 생성할 수도 있습니다. 이러한 조사 결과가 유용하지 않으면 숨길 수 있습니다.

데이터를 저장 시 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. RDS 스냅샷의 데이터는 추가 보안 계층을 위해 저장 시 암호화되어야 합니다.

문제 해결

RDS 스냅샷을 암호화하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 암호화를 참조하세요. RDS DB 인스턴스를 암호화하면 암호화된 데이터에는 인스턴스의 기본 스토리지, 자동 백업, 읽기 전용 복제본 및 스냅샷이 포함됩니다.

RDS DB 인스턴스를 생성할 때만 암호화할 수 있으며, DB 인스턴스가 생성된 후에는 암호화할 수 없습니다. 다만 암호화되지 않은 스냅샷의 사본을 암호화할 수 있기 때문에 암호화되지 않은 DB 인스턴

스에 실질적으로 암호화를 추가할 수 있습니다. 즉, DB 인스턴스의 스냅샷을 만든 다음 해당 스냅샷의 암호화된 사본을 만들 수 있습니다. 그런 다음 암호화된 스냅샷에서 DB 인스턴스를 복구할 수 있고, 원본 DB 인스턴스의 암호화된 사본이 생깁니다.

[RDS.5] RDS DB 인스턴스는 여러 가용 영역으로 구성해야 합니다.

관련 요구 사항: CIS AWS Foundations 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-multi-az-support`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 RDS DB 인스턴스에 대해 고가용성이 활성화되었는지 여부를 확인합니다. RDS DB 인스턴스가 여러 가용 영역(AZ)에 구성되지 않으면 제어가 실패합니다. 이 제어는 다중 AZ DB 클러스터 배포의 일부인 RDS DB 인스턴스에는 적용되지 않습니다.

Amazon RDS DB 인스턴스를 AZs로 구성하면 저장된 데이터의 가용성을 보장하는 데 도움이 됩니다. 다중 AZ 배포를 사용하면 AZ 가용성에 문제가 있거나 정기적인 RDS 유지 관리 중에 문제가 있는 경우, 자동 장애 조치가 가능합니다.

문제 해결

다중 AZ에 DB 인스턴스를 배포하려면 Amazon RDS 사용 설명서의 DB 인스턴스를 다중 AZ DB 인스턴스 배포로 수정을 참조하세요.

[RDS.6] RDS DB 인스턴스에 대한 Enhanced Monitoring을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-enhanced-monitoring-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `monitoringInterval` | 모니터링 메트릭 수집 간격(초) | Enum | `1`, `5`, `10`, `15`, `30`, `60` | 기본값 없음 | |

이 제어는 Amazon Relational Database Service(RDS) DB 인스턴스에 확장 모니터링이 활성화되었는지 확인합니다. 인스턴스에 대해 향상된 모니터링이 활성화되지 않은 경우, 제어가 실패합니다. `monitoringInterval` 파라미터에 사용자 지정 값을 제공하는 경우, 인스턴스에 대해 지정된 간격으로 향상된 모니터링 메트릭이 수집되는 경우에만 제어가 통과합니다.

Amazon RDS에서는 Enhanced Monitoring을 통해 기본 인프라의 성능 변화에 더욱 신속하게 대응할 수 있습니다. 이러한 성능 변화로 인해 데이터 가용성이 부족해질 수 있습니다. Enhanced Monitoring은 RDS DB 인스턴스가 실행되는 운영 체제에 대한 실시간 메트릭를 제공합니다. 에이전트가 인스턴스에 설치되어 있습니다. 에이전트는 하이퍼바이저 계층에서 가능한 것보다 더 정확하게 메트릭를 얻을 수 있습니다.

Enhanced Monitoring 메트릭는 DB 인스턴스의 다양한 프로세스나 스레드가 CPU를 어떻게 사용하는지 확인하려는 경우, 유용합니다. 자세한 내용을 알아보려면 Amazon RDS 사용 설명서의 Enhanced Monitoring을 참조하세요.

문제 해결

DB 인스턴스의 Enhanced Monitoring을 활성화하는 방법에 대한 자세한 지침은 Amazon RDS 사용 설명서의 Enhanced Monitoring 설정 및 활성화를 참조하세요.

[RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 클러스터에 삭제 보호가 활성화되어 있는지 확인합니다. RDS DB 클러스터에 삭제 방지 기능이 활성화되지 않은 경우, 제어가 실패합니다.

이 제어는 RDS DB 인스턴스용입니다. 하지만 Aurora DB 인스턴스, Neptune DB 인스턴스 및 Amazon DocumentDB 클러스터에 대한 조사 결과를 생성할 수도 있습니다. 이러한 조사 결과가 유용하지 않으면 숨길 수 있습니다.

클러스터 삭제 보호를 활성화하면 우발적인 데이터베이스 삭제 또는 승인되지 않은 개체에 의한 삭제에 대한 추가 보호 계층이 제공됩니다.

삭제 방지 기능이 활성화되면 RDS 클러스터가 삭제될 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 보호를 비활성화해야 합니다.

문제 해결

RDS DB 클러스터에 대한 삭제 보호를 활성화하려면 Amazon RDS 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하세요. 삭제 방지에서 삭제 방지 활성화를 선택합니다.

[RDS.8] RDS DB 인스턴스에는 삭제 방지 기능이 활성화되어 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5(2), NIST.800-53.r5 SI-13(5)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-deletion-protection-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

- `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`(사용자 지정할 수 없음)

이 제어는 나열된 데이터베이스 엔진 중 하나를 사용하는 RDS DB 인스턴스에 삭제 보호가 활성화되어 있는지 확인합니다. RDS DB 인스턴스에 삭제 방지 기능이 활성화되지 않은 경우, 제어가 실패합니다.

인스턴스 삭제 보호를 활성화하면 우발적인 데이터베이스 삭제 또는 승인되지 않은 개체에 의한 삭제에 대한 추가 보호 계층이 제공됩니다.

삭제 보호가 활성화되어 있는 동안에는 RDS DB 인스턴스를 삭제할 수 없습니다. 삭제 요청이 성공하려면 먼저 삭제 보호를 비활성화해야 합니다.

문제 해결

RDS DB 인스턴스에 대한 삭제 보호를 활성화하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하세요. 삭제 방지에서 삭제 방지 활성화를 선택합니다.

[RDS.9] RDS DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS DB 인스턴스가 Amazon CloudWatch Logs에 다음 로그를 게시하도록 구성되어 있는지 여부를 확인합니다. 인스턴스가 다음 로그를 CloudWatch Logs에 게시하도록 구성되지 않으면 제어가 실패합니다.

- Oracle: Alert, Audit, Trace, Listener
- PostgreSQL: Postgresql, Upgrade
- MySQL: Audit, Error, General, SlowQuery
- MariaDB: Audit, Error, General, SlowQuery
- SQL Server: Error, Agent
- Aurora-MySQL: Audit, Error, General, SlowQuery
- Aurora-PostgreSQL: Postgresql

RDS 데이터베이스에는 관련 로그가 활성화되어 있어야 합니다. 데이터베이스 로깅은 RDS에 대한 요청에 대한 자세한 기록을 제공합니다. 데이터베이스 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다.

문제 해결

RDS 데이터베이스 로그를 CloudWatch Logs에 게시하는 방법에 대한 자세한 내용은 Amazon RDS 사용 설명서의 CloudWatch Logs에 게시할 로그 지정을 참조하세요.

[RDS.10] RDS 인스턴스에 대해 IAM 인증을 구성해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-iam-authentication-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 인스턴스에 IAM 데이터베이스 인증이 활성화되어 있는지 확인합니다. RDS DB 인스턴스에 대해 IAM 인증이 구성되지 않은 경우, 제어가 실패합니다. 이 제어는 엔진 유형이 `mysql`, `postgres`, `aurora`, `aurora-mysql`, `aurora-postgresql` 및 `mariadb`인 RDS 인스턴스만 평가합니다. 또한 검색 조사 결과가 생성되려면 RDS 인스턴스가 `available`,`backing-up`, `storage-optimization` 또는 `storage-full` 상태 중 하나여야 합니다.

IAM 데이터베이스 인증을 사용하면 암호 대신 인증 토큰을 사용하여 데이터베이스 인스턴스를 인증할 수 있습니다. 데이터베이스를 오가는 네트워크 트래픽은 SSL을 통해 암호화됩니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 IAM 데이터베이스 인증을 참조하세요.

문제 해결

RDS DB 인스턴스에서 IAM 데이터베이스 인증을 활성화하려면 Amazon RDS 사용 설명서의 IAM 데이터베이스 인증 활성화 및 비활성화를 참조하세요.

[RDS.11] RDS 인스턴스에는 자동 백업이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `db-instance-backup-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `backupRetentionMinimum` | 백업 보존 기간(일수) | Integer | 7~35 | 7 | |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `checkReadReplicas` | RDS DB 인스턴스에 읽기 전용 복제본 백업이 활성화되어 있는지 확인합니다. | 부울 | 사용자 지정할 수 없음 | `false` | |

이 제어는 Amazon Relational Database Service 인스턴스에 자동 백업이 활성화되어 있고 백업 보존 기간이 지정된 기간 이상인지 확인합니다. 읽기 전용 복제본은 평가에서 제외됩니다. 인스턴트에 대한 백업이 활성화되지 않았거나 보존 기간이 지정된 기간 미만인 경우, 제어가 실패합니다. 백업 보존 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있고 시스템의 복원력을 강화할 수 있습니다. Amazon RDS를 사용하면 일일 전체 인스턴스 볼륨 스냅샷을 구성할 수 있습니다. Amazon RDS 자동 백업에 대한 자세한 내용은 Amazon RDS 사용 설명서의 백업 작업을 참조하세요.

문제 해결

RDS DB 인스턴스에서 자동 백업을 활성화하려면 Amazon RDS 사용 설명서의 자동 백업 활성화를 참조하세요.

[RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 비밀번호 없는 인증

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-iam-authentication-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS DB 클러스터에 IAM 데이터베이스 인증이 활성화되어 있는지 확인합니다.

IAM 데이터베이스 인증을 사용하면 데이터베이스 인스턴스에 암호 없이 인증할 수 있습니다. 인증은 인증 토큰을 사용합니다. 데이터베이스를 오가는 네트워크 트래픽은 SSL을 통해 암호화됩니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 IAM 데이터베이스 인증을 참조하세요.

문제 해결

DB 클러스터에 대한 IAM 인증을 활성화하려면 Amazon Aurora 사용 설명서의 IAM 데이터베이스 인증 활성화 및 비활성화를 참조하세요.

[RDS.13] RDS 자동 마이너 버전 업그레이드를 활성화해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.2.2, CIS AWS 파운데이션 벤치마크 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-automatic-minor-version-upgrade-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS DB 인스턴스에 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. RDS DB 인스턴스에 대해 자동 마이너 버전 업그레이드를 활성화하지 않으면 제어가 실패합니다.

> **Note**
>
> 이 제어는 각 Amazon RDS DB 인스턴스를 독립적으로 평가합니다. Amazon Aurora 클러스터의 경우 자동 마이너 버전 업그레이드를 사용하려면 클러스터에서이 설정을 활성화해야 합니다. 클러스터의 모든 인스턴스에서도이 설정을 활성화해야 합니다. 개별 인스턴스에 대한 `PASSED` 조사 결과는 클러스터 수준에서 설정을 활성화하지 않은 경우 업그레이드가 발생한다는 것을 보장하지 않습니다.
> 또한이 제어는 자동 마이너 버전 업그레이드를 지원하지 않는 구성을 고려하지 않습니다. 여기에는 Aurora 글로벌 데이터베이스의 Aurora 클러스터와 리전 간 읽기 전용 복제본이 있는

Aurora MySQL 클러스터가 포함됩니다. 이러한 구성의 경우 제어는 실제 업그레이드 동작을 정확하게 반영하지 않는 평가 결과를 생성할 수 있습니다.

마이너 버전 자동 업그레이드는 데이터베이스를 최신 데이터베이스 엔진 버전으로 주기적으로 업데이트합니다. 그러나 업그레이드에 항상 최신 데이터베이스 엔진 버전이 포함되는 것은 아닙니다. 특정 시간에 데이터베이스를 특정 버전으로 유지해야 하는 경우 필요한 일정에 따라 필요한 데이터베이스 버전으로 수동으로 업그레이드하는 것이 좋습니다. 중요한 보안 문제가 발생하거나 버전이 지원 종료에 도달하면 마이너 버전 자동 업그레이드 옵션을 활성화하지 않은 경우에도 Amazon RDS에 마이너 버전 업그레이드가 적용될 수 있습니다. 자세한 내용은 특정 데이터베이스 엔진에 대한 Amazon RDS 업그레이드 설명서를 참조하세요.

- RDS for MariaDB의 마이너 버전 자동 업그레이드
- RDS for MySQL의 마이너 버전 자동 업그레이드
- RDS for PostgreSQL의 마이너 버전 자동 업그레이드
- Amazon RDS 버전의 Db2
- Oracle 마이너 버전 업그레이드
- Microsoft SQL Server DB 엔진 업그레이드

문제 해결

기존 DB 인스턴스의 자동 마이너 버전 업그레이드를 활성화하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하세요. 자동 마이너 버전 업그레이드의 경우, 예를 선택합니다.

[RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `aurora-mysql-backtracking-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `BacktrackWindowInHours` | Aurora MySQL 클러스터를 역추적하는 데 걸리는 기간(시간) | 배정밀도 실수 | `0.1~72` | 기본값 없음 | |

이 제어는 Amazon Aurora 클러스터에 역추적이 활성화되어 있는지 확인합니다. 클러스터에 역추적이 활성화되지 않은 경우, 제어가 실패합니다. `BacktrackWindowInHours` 파라미터에 사용자 지정 값을 제공하는 경우 지정된 시간 동안 클러스터를 역추적하는 경우에만 제어가 통과합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있습니다. 또한 시스템의 복원력을 강화합니다. Aurora 역추적은 데이터베이스를 특정 시점으로 복구하는 데 걸리는 시간을 줄여줍니다. 이를 위해 데이터베이스를 복원할 필요는 없습니다.

문제 해결

Aurora 역추적을 활성화하려면 Amazon Aurora 사용 설명서의 역추적 구성을 참조하세요.

기존 클러스터에서는 역추적을 활성화할 수 없다는 점에 유의하세요. 대신 역추적이 활성화된 복제본을 생성할 수 있습니다. Aurora 역추적 제한 사항에 대한 자세한 내용은 역추적 개요의 제한 사항 목록을 참조하세요.

[RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.

관련 요구 사항: CIS AWS Foundations 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)

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-multi-az-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 컨트롤은 RDS DB 클러스터에 대해 고가용성이 활성화되었는지 여부를 확인합니다. RDS DB 클러스터가 여러 가용 영역(AZ)에 배포되지 않으면 제어가 실패합니다.

저장된 데이터의 가용성을 보장하려면 여러 AZ에 대해 RDS DB 클러스터를 구성해야 합니다. 여러 AZ에 배포하면 AZ 가용성 문제가 발생하는 경우 및 정기적인 RDS 유지 관리 이벤트 중에 자동 장애 조치가 가능합니다.

문제 해결

다중 AZ에 DB 클러스터를 배포하려면 Amazon RDS 사용 설명서의 DB 인스턴스를 다중 AZ DB 인스턴스 배포로 수정을 참조하세요.

Aurora 글로벌 데이터베이스에 대한 수정 단계가 다릅니다. Aurora 글로벌 데이터베이스에 대해 여러 가용 영역을 구성하려면 DB 클러스터를 선택합니다. 그런 다음 작업과 리더 추가를 선택하고 여러 AZ를 지정합니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 DB 클러스터에 Aurora 복제본 추가를 참조하세요.

[RDS.16] Aurora DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-copy-tags-to-snapshots-enabled` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Aurora DB 클러스터가 DB 클러스터의 스냅샷이 생성될 때 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다. Aurora DB 클러스터가 클러스터의 스냅샷이 생성될 때 스냅샷에 태그를 자동으로 복사하도록 구성되지 않은 경우 제어가 실패합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 보안 태세를 평가하고 잠재적인 취약 영역에 조치를 취할 수 있도록 모든 Amazon Aurora DB 클러스터에 대한 가시성을 확보해야 합니다. Aurora DB 스냅샷은 상위 DB 클러스터와 동일한 태그가 지정되어야 합니다. Amazon Aurora에서는 클러스터의 모든 태그를 클러스터의 스냅샷에 자동으로 복사하도록 DB 클러스터를 구성할 수 있습니다. 이 설정을 활성화하면 DB 스냅샷이 상위 DB 클러스터와 동일한 태그를 상속하게 됩니다.

문제 해결

DB 스냅샷에 태그를 자동으로 복사하도록 Amazon Aurora DB 클러스터를 구성하는 방법에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora DB 클러스터 수정을 참조하세요.

[RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2(2)

범주: 식별 > 인벤토리

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-copy-tags-to-snapshots-enabled` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 스냅샷이 생성될 때 RDS DB 인스턴스가 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다.

IT 자산의 식별 및 인벤토리는 거버넌스 및 보안의 중요한 측면입니다. 보안 상태를 평가하고 잠재적인 약점 영역에 조치를 취할 수 있도록 모든 RDS DB 인스턴스에 대한 가시성을 확보해야 합니다. 스냅샷에는 상위 RDS 데이터베이스 인스턴스와 같은 방식으로 태그를 지정해야 합니다. 이 설정을 활성화하면 스냅샷이 상위 데이터베이스 인스턴스의 태그를 상속하게 됩니다.

문제 해결

RDS DB 인스턴스의 스냅샷에 태그를 자동으로 복사하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하세요. 스냅샷으로 태그 복사를 선택합니다.

[RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-cluster-event-notifications-configured` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 데이터베이스 클러스터에 대한 기존 Amazon RDS 이벤트 구독에 다음 소스 유형 및 이벤트 범주 키-값 쌍에 대해 사용하도록 설정된 알림이 있는지 확인합니다.

```
DBCluster: ["maintenance","failure"]
```

계정에 기존 이벤트 구독이 없는 경우, 제어가 통과됩니다.

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하세요.

문제 해결

RDS 클러스터 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 소스 유형 | 클러스터 |
| 포함할 클러스터 | 모든 클러스터 |
| 포함할 이벤트 범주 | 특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다. |

[RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-instance-event-notifications-configured` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 데이터베이스 인스턴스에 대한 기존 Amazon RDS 이벤트 구독에 다음 소스 유형 및 이벤트 범주 키-값 쌍에 대해 사용하도록 설정된 알림이 있는지 확인합니다.

```
DBInstance: ["maintenance","configuration change","failure"]
```

계정에 기존 이벤트 구독이 없는 경우, 제어가 통과됩니다.

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하세요.

문제 해결

RDS 인스턴스 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 소스 유형 | 인스턴스 |
| 포함할 인스턴스 | 모든 인스턴스 |
| 포함할 이벤트 범주 | 특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다. |

[RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-pg-event-notifications-configured` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 다음과 같은 소스 유형, 이벤트 범주 키-값 쌍에 대해 알림이 활성화된 상태에서 Amazon RDS 이벤트 구독이 존재하는지 확인합니다. 계정에 기존 이벤트 구독이 없는 경우, 제어가 통과됩니다.

```
DBParameterGroup: ["configuration change"]
```

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하세요.

문제 해결

RDS 데이터베이스 파라미터 그룹 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 소스 유형 | 파라미터 그룹 |
| 포함할 파라미터 그룹 | 모든 파라미터 그룹 |
| 포함할 이벤트 범주 | 특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다. |

[RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, PCI DSS v4.0.1/11.5.2

범주: 감지 > 감지 서비스 > 애플리케이션 모니터링

심각도: 낮음

리소스 유형: `AWS::RDS::EventSubscription`

AWS Config 규칙: `rds-sg-event-notifications-configured` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 다음과 같은 소스 유형, 이벤트 범주 키-값 쌍에 대해 알림이 활성화된 상태에서 Amazon RDS 이벤트 구독이 존재하는지 확인합니다. 계정에 기존 이벤트 구독이 없는 경우, 제어가 통과됩니다.

```
DBSecurityGroup: ["configuration change","failure"]
```

RDS 이벤트 알림은 Amazon SNS를 사용하여 RDS 리소스의 가용성 또는 구성 변경 사항을 알려줍니다. 이러한 알림을 통해 신속하게 대응할 수 있습니다. RDS 이벤트 알림에 대한 추가 정보는 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 사용을 참조하세요.

문제 해결

RDS 인스턴스 이벤트 알림을 구독하려면 Amazon RDS 사용 설명서의 Amazon RDS 이벤트 알림 구독을 참조하세요. 다음 값을 사용합니다.

| Field | 값 |
| --- | --- |
| 소스 유형 | 보안 그룹 |
| 포함해야 할 보안 그룹 | 모든 보안 그룹 |
| 포함할 이벤트 범주 | 특정 이벤트 범주 또는 모든 이벤트 범주를 선택합니다. |

[RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-no-default-ports` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS 클러스터 또는 인스턴스가 데이터베이스 엔진의 기본 포트가 아닌 다른 포트를 사용하는지 여부를 확인합니다. RDS 클러스터 또는 인스턴스가 기본 포트를 사용하는 경우, 제어가 실패합니다. 이 제어는 클러스터의 멤버인 RDS 인스턴스에는 적용되지 않습니다.

알려진 포트를 사용하여 RDS 클러스터 또는 인스턴스를 배포하면 공격자가 클러스터 또는 인스턴스에 대한 정보를 추측할 수 있습니다. 공격자는 이 정보를 다른 정보와 함께 사용하여 RDS 클러스터 또는 인스턴스에 연결하거나 애플리케이션에 대한 추가 정보를 얻을 수 있습니다.

포트를 변경할 때는 이전 포트에 연결하는 데 사용된 기존 연결 문자열도 업데이트해야 합니다. 또한 DB 인스턴스의 보안 그룹에 새로운 포트에서의 연결을 허용하는 인그레스 규칙이 포함되어 있는지 확인해야 합니다.

문제 해결

기존 RDS DB 인스턴스의 기본 포트를 수정하려면 Amazon RDS 사용 설명서의 Amazon RDS DB 인스턴스 수정을 참조하세요. 기존 RDS DB 클러스터의 기본 포트를 수정하려면 Amazon Aurora 사용 설명서의 콘솔, CLI 및 API를 사용하여 DB 클러스터 수정을 참조하세요. 데이터베이스 포트의 경우, 포트 값을 기본값이 아닌 값으로 변경하세요.

[RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.2

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-default-admin-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS 데이터베이스 클러스터가 관리자 사용자 이름을 기본값에서 변경했는지 여부를 확인합니다. 이 제어는 neptune(Neptune DB) 또는 docdb(DocumentDB) 유형의 엔진에는 적용되지 않습니다. 관리자 사용자 이름을 기본값으로 설정하면 이 규칙이 실패합니다.

Amazon RDS 데이터베이스를 생성할 때는 기본 관리자 사용자 이름을 고유한 값으로 변경해야 합니다. 기본 사용자 이름은 공개되어 있으므로 RDS 데이터베이스 생성 중에 변경해야 합니다. 기본 사용자 이름을 변경하면 의도하지 않은 액세스의 위험이 줄어듭니다.

문제 해결

Amazon RDS 데이터베이스 클러스터와 연결된 관리자 사용자 이름을 변경하려면 데이터베이스를 생성할 때 새로운 RDS 데이터베이스 클러스터를 생성하고 기본 관리자 사용자 이름을 변경하세요.

[RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, PCI DSS v4.0.1/2.2.2

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-instance-default-admin-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Relational Database Service(RDS) 데이터베이스 인스턴스의 관리자 사용자 이름을 기본값에서 변경했는지 여부를 확인합니다. 관리자 사용자 이름이 기본값으로 설정된 경우, 제어가 실패합니다. 이 제어는 neptune(Neptune DB) 또는 docdb(DocumentDB) 유형의 엔진과 클러스터의 멤버인 RDS 인스턴스에는 적용되지 않습니다.

Amazon RDS 데이터베이스의 기본 관리 사용자 이름은 공개된 정보입니다. Amazon RDS 데이터베이스를 생성할 때는 기본 관리자 사용자 이름을 고유한 값으로 변경하여 의도하지 않은 액세스의 위험을 줄여야 합니다.

문제 해결

RDS 데이터베이스 인스턴스와 관련된 관리 사용자 이름을 변경하려면 먼저 새로운 RDS 데이터베이스 인스턴스를 생성하세요. 데이터베이스를 생성할 때 기본 관리 사용자 이름을 변경하세요.

[RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.

범주: 복구 > 복원력 > 백업 활성화

관련 요구 사항: 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)

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: `rds-resources-protected-by-backup-plan`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `backupVaultLockCheck` | 파라미터가 true로 설정되고 리소스가 AWS Backup 볼트 잠금을 사용하는 경우 제어가 `PASSED` 결과를 생성합니다. | 부울 | `true` 또는 `false` | 기본값 없음 | |

이 제어는 Amazon RDS DB 인스턴스에 백업 계획이 적용되는지 여부를 평가합니다. RDS DB 인스턴스에 백업 계획이 적용되지 않는 경우, 이 제어가 실패합니다. `backupVaultLockCheck` 파라미터를

와 동일하게 설정하면 인스턴스`true`가 AWS Backup 잠긴 볼트에 백업된 경우에만 제어가 전달됩니다.

> **Note**
>
> 이 제어는 Neptune 및 DocumentDB 인스턴스를 평가하지 않습니다. 또한 클러스터의 멤버인 RDS DB 인스턴스도 평가하지 않습니다.

AWS Backup 는 데이터 백업을 중앙 집중화하고 자동화하는 완전 관리형 백업 서비스입니다 AWS 서비스. 를 사용하면 백업 계획이라고 하는 백업 정책을 생성할 AWS Backup수 있습니다. 이러한 계획을 사용하여 데이터 백업 빈도 및 백업 보존 기간과 같은 백업 요구 사항을 정의할 수 있습니다. 백업 계획에 RDS DB 인스턴스를 포함하면 의도하지 않은 손실이나 삭제로부터 데이터를 보호하는 데 도움이 됩니다.

문제 해결

AWS Backup 백업 계획에 RDS DB 인스턴스를 추가하려면 AWS Backup 개발자 안내서의 백업 계획에 리소스 할당을 참조하세요.

[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-encrypted-at-rest`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 RDS DB 클러스터가 저장 시 암호화되어 있는지 확인합니다. RDS DB 클러스터가 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 암호화를 사용하면 해당 데이터의 기밀성을 보호하여 권한 없는 사용자가 해당 데이터에 액세스할 수 있는 위

험을 줄일 수 있습니다. RDS DB 클러스터를 암호화하면 데이터와 메타데이터를 무단 액세스로부터 보호할 수 있습니다. 또한 프로덕션 파일 시스템의 미사용 데이터 암호화에 대한 규정 준수 요구 사항도 충족합니다.

문제 해결

RDS DB 클러스터를 만들 때 저장 시 암호화를 활성화할 수 있습니다. 클러스터를 생성한 후에는 암호화 설정을 변경할 수 없습니다. 자세한 내용을 알아보려면 Amazon Aurora 사용 설명서의 Amazon Aurora DB 클러스터 암호화를 참조하세요.

[RDS.28] RDS DB 클러스터에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙:`tagged-rds-dbcluster` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon RDS DB 클러스터에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. DB 클러스터에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 DB 클러스터에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리,

검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

RDS DB 클러스터에 태그를 추가하려면Amazon RDS 사용 설명서의 Amazon RDS 리소스 태깅을 참조하세요.

[RDS.29] RDS DB 클러스터 스냅샷에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBClusterSnapshot`

AWS Config 규칙:`tagged-rds-dbclustersnapshot` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon RDS DB 클러스터 스냅샷에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. DB 클러스터 스냅샷에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 DB 클러스터 스냅샷에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

RDS DB 클러스터 스냅샷에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태깅을 참조하세요.

[RDS.30] RDS DB 인스턴스에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙:`tagged-rds-dbinstance` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| requiredTagKeys | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon RDS DB 인스턴스에 파라미터 requiredTagKeys에 정의된 특정 키가 있는 태그가 있는지 확인합니다. DB 인스턴스에 태그 키가 없거나 파라미터 requiredTagKeys에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 requiredTagKeys이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 DB 인스턴스에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 aws:로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

RDS DB 인스턴스에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하세요.

[RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::RDS::DBSecurityGroup`

AWS Config 규칙:`tagged-rds-dbsecuritygroup` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon RDS DB 보안 그룹에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. DB 보안 그룹에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 DB 보안 그룹에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

RDS DB 보안 그룹에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하세요.

[RDS.32] RDS DB 스냅샷에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::RDS::DBSnapshot`

AWS Config 규칙:`tagged-rds-dbsnapshot` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon RDS DB 스냅샷에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. DB 스냅샷에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 DB 스냅샷에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할

수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

RDS DB 스냅샷에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하세요.

[RDS.33] RDS DB 서브넷 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::RDS::DBSubnetGroup`

AWS Config 규칙:`tagged-rds-dbsubnetgroups` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon RDS DB 서브넷 그룹에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. DB 서브넷 그룹에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된

모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 DB 서브넷에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS 리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS 리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까 AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다 AWS Billing. 태그 지정 모범 사례는의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

RDS DB 서브넷 그룹에 태그를 추가하려면 Amazon RDS 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하세요.

[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-aurora-mysql-audit-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Aurora MySQL DB 클러스터가 Amazon CloudWatch Logs에 감사 로그를 게시하는지 여부를 확인합니다. 클러스터가 CloudWatch Logs에 감사 로그를 게시하도록 구성되지 않은 경우, 제어가 실패합니다. 제어는 Aurora Serverless v1 DB 클러스터에 대한 조사 결과를 생성하지 않습니다.

감사 로그는 로그인 시도, 데이터 수정, 스키마 변경 및 보안 및 규정 준수를 위해 감사할 수 있는 기타 이벤트를 포함한 데이터베이스 활동 기록을 캡처합니다. Amazon CloudWatch Logs의 로그 그룹에 감사 로그를 게시하도록 Aurora MySQL DB 클러스터를 구성하면 로그 데이터에 대한 실시간 분석을 수행할 수 있습니다. CloudWatch Logs는 내구성이 뛰어난 스토리지에 로그를 유지합니다. CloudWatch에서 경보를 생성하고 메트릭를 볼 수도 있습니다.

> **Note**
>
> 감사 로그를 CloudWatch Logs에 게시하는 다른 방법은 고급 감사를 활성화하고 클러스터 수준의 DB 파라미터 `server_audit_logs_upload`를 `1`로 설정하는 것입니다. `server_audit_logs_upload parameter`의 기본값은 `0`입니다. 그러나 이 제어를 통과하려면 대신 다음 수정 지침을 사용하는 것이 좋습니다.

문제 해결

Aurora MySQL DB 클러스터 감사 로그를 CloudWatch Logs에 게시하려면 Amazon Aurora 사용 설명서의 Amazon CloudWatch Logs에 Amazon Aurora MySQL 로그 게시를 참조하세요.

[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: `rds-cluster-auto-minor-version-upgrade-enable`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Aurora DB 클러스터를 포함한 Amazon RDS DB 클러스터에 대해 자동 마이너 버전 업그레이드가 활성화되어 있는지 확인합니다. DB 클러스터에 대해 자동 마이너 버전 업그레이드가 활성화되지 않은 경우 제어가 실패합니다.

마이너 버전 자동 업그레이드를 사용하면 DB 클러스터를 최신 상태로 유지할 수 있습니다. 마이너 버전은 새로운 소프트웨어 기능, 버그 수정, 보안 패치 및 성능 개선을 도입할 수 있습니다. RDS 데이터베이스 클러스터에서 자동 마이너 버전 업그레이드를 활성화하면 클러스터는 새로운 버전이 출시될 때 클러스터의 인스턴스와 함께 마이너 버전에 대한 자동 업데이트를 받게 됩니다. 업데이트는 유지 관리 기간 동안 자동으로 적용됩니다.

문제 해결

다중-AZ DB 클러스터에서 자동 마이너 버전 업그레이드를 활성화하려면 Amazon RDS 사용 설명서의 다중-AZ DB 클러스터 수정을 참조하세요.

Aurora DB 클러스터에서 마이너 버전 자동 업그레이드를 활성화하려면 Amazon Aurora 사용 설명서의 Amazon Aurora DB 클러스터 수정을 참조하세요.

[RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/10.4.2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: rds-postgresql-logs-to-cloudwatch

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `logTypes` | CloudWatch Logs에 게시할 로그 유형의 쉼표로 구분된 목록 | StringList | 사용자 지정할 수 없음 | `postgresql` |

이 제어는 Amazon RDS for PostgreSQL DB 인스턴스가 Amazon CloudWatch Logs에 다음 로그를 게시하도록 구성되어 있는지 여부를 확인합니다. `logTypes` 파라미터에 언급된 로그 유형을 CloudWatch Logs에 게시하도록 PostgreSQL DB 인스턴스가 구성되지 않은 경우, 제어가 실패합니다.

데이터베이스 로깅은 RDS 인스턴스에 대한 요청에 대한 자세한 기록을 제공합니다. PostgreSQL은 관리자를 위한 유용한 정보를 포함하는 이벤트 로그 파일을 생성합니다. 이러한 로그를 CloudWatch Logs에 게시하면 로그 관리를 중앙 집중화하고 로그 데이터에 대한 실시간 분석을 수행하는 데 도움이 됩니다. CloudWatch Logs는 내구성이 뛰어난 스토리지에 로그를 유지합니다. CloudWatch에서 경보를 생성하고 메트릭를 볼 수도 있습니다.

문제 해결

PostgreSQL DB 인스턴스 로그를 CloudWatch Logs에 게시하려면 Amazon RDS 사용 설명서의 Amazon CloudWatch Logs에 PostgreSQL 로그 게시를 참조하세요.

[RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/10.4.2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: rds-aurora-postgresql-logs-to-cloudwatch

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Aurora PostgreSQL DB 클러스터가 Amazon CloudWatch Logs에 로그를 게시하는지 여부를 확인합니다. Aurora PostgreSQL 클러스터가 CloudWatch Logs에 PostgreSQL 로그를 게시하도록 구성되지 않은 경우, 제어가 실패합니다.

데이터베이스 로깅은 RDS 클러스터에 대한 요청에 대한 자세한 기록을 제공합니다. Aurora PostgreSQL은 관리자를 위한 유용한 정보를 포함하는 이벤트 로그 파일을 생성합니다. 이러한 로그를 CloudWatch Logs에 게시하면 로그 관리를 중앙 집중화하고 로그 데이터에 대한 실시간 분석을 수행하는 데 도움이 됩니다. CloudWatch Logs는 내구성이 뛰어난 스토리지에 로그를 유지합니다. CloudWatch에서 경보를 생성하고 메트릭를 볼 수도 있습니다.

문제 해결

Aurora PostgreSQL DB 인스턴스 로그를 CloudWatch Logs에 게시하려면 Amazon RDS 사용 설명서의 Amazon CloudWatch Logs에 PostgreSQL 로그 게시를 참조하세요.

[RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: rds-postgres-instance-encrypted-in-transit

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon RDS for PostgreSQL 데이터베이스(DB) 인스턴스에 대한 연결이 전송 중에 암호화되는지 확인합니다. 인스턴스와 연결된 파라미터 그룹의 `rds.force_ssl` 파라미터가 `0`(꺼짐)으로 설정된 경우 제어가 실패합니다. 이 제어는 DB 클러스터의 멤버인 RDS DB 인스턴스를 평가하지 않습니다.

전송 중 데이터는 클러스터의 노드 사이 또는 클러스터와 애플리케이션 사이와 같이 한 위치에서 다른 위치로 이동하는 데이터를 나타냅니다. 데이터는 인터넷 또는 프라이빗 네트워크 내에서 이동할 수 있습니다. 전송 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다.

문제 해결

RDS for PostgreSQL DB 인스턴스에 대한 모든 연결이 SSL을 사용하도록 요구하려면 Amazon RDS 사용 설명서의 PostgreSQL DB 인스턴스와 함께 SSL 사용을 참조하세요.

[RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: rds-mysql-instance-encrypted-in-transit

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon RDS for MySQL 데이터베이스(DB) 인스턴스에 대한 연결이 전송 중에 암호화되는지 확인합니다. 인스턴스와 연결된 파라미터 그룹의 `rds.require_secure_transport` 파라미터가 `0`(꺼짐)으로 설정된 경우 제어가 실패합니다. 이 제어는 DB 클러스터의 멤버인 RDS DB 인스턴스를 평가하지 않습니다.

전송 중 데이터는 클러스터의 노드 사이 또는 클러스터와 애플리케이션 사이와 같이 한 위치에서 다른 위치로 이동하는 데이터를 나타냅니다. 데이터는 인터넷 또는 프라이빗 네트워크 내에서 이동할 수 있습니다. 전송 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다.

문제 해결

RDS for MySQL DB 인스턴스에 대한 모든 연결이 SSL을 사용하도록 요구하려면 Amazon RDS 사용 설명서의 Amazon RDS의 MySQL DB 인스턴스에 대한 SSL/TLS 지원을 참조하세요.

[RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: rds-sql-server-logs-to-cloudwatch

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `logTypes` | RDS for SQL Server DB 인스턴스가 CloudWatch Logs에 게 | EnumList(최대 2개 항목) | `agent`, `error` | `agent`, `error` |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 시하도록 구성해야 하는 로그 유형의 목록입니다. DB 인스턴스가 이 목록에 지정된 유형의 로그를 게시하도록 구성되지 않은 경우 이 제어가 실패합니다. | | | |

이 제어는 Amazon RDS for Microsoft SQL Server DB 인스턴스가 다음 로그를 Amazon CloudWatch Logs에 게시하도록 구성되어 있는지 확인합니다. RDS for SQL Server DB 인스턴스가 다음 로그를 CloudWatch Logs에 게시하도록 구성되지 않은 경우 제어가 실패합니다. 선택적으로 DB 인스턴스가 게시하도록 구성해야 하는 로그 유형을 지정할 수 있습니다.

데이터베이스 로깅은 RDS DB 인스턴스에 대한 요청의 자세한 레코드를 제공합니다. CloudWatch Logs에 로그를 게시하면 로그 관리를 중앙 집중화하고 로그 데이터에 대한 실시간 분석을 수행하는 데 도움이 됩니다. CloudWatch Logs는 내구성이 뛰어난 스토리지에 로그를 유지합니다. 또한 이를 사용하여 오류 로그에 기록된 빈번한 재시작과 같은 발생할 수 있는 특정 오류에 대한 경보를 생성할 수 있습니다. 마찬가지로, SQL 에이전트 작업과 관련된 SQL Server 에이전트 로그에 기록된 오류 또는 경고에 대한 경보를 생성할 수 있습니다.

문제 해결

RDS for SQL Server DB 인스턴스의 로그를 CloudWatch Logs에 게시하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 Amazon RDS for Microsoft SQL Server 데이터베이스 로그 파일을 참조하세요.

[RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: rds-sqlserver-encrypted-in-transit

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon RDS for Microsoft SQL Server DB 인스턴스에 대한 연결이 전송 중 암호화되는지 확인합니다. DB 인스턴스와 연결된 파라미터 그룹의 `rds.force_ssl` 파라미터가 `0 (off)`으로 설정된 경우 제어가 실패합니다.

전송 중 데이터는 DB 클러스터의 노드 사이 또는 DB 클러스터와 클라이언트 애플리케이션 사이와 같이 한 위치에서 다른 위치로 이동하는 데이터를 나타냅니다. 데이터는 인터넷을 통해 또는 프라이빗 네트워크 내에서 이동할 수 있습니다. 전송 중 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다.

문제 해결

Microsoft SQL Server를 실행하는 Amazon RDS DB 인스턴스에 연결하기 위해 SSL/TLS를 활성화하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 Microsoft SQL Server DB 인스턴스와 함께 SSL 사용을 참조하세요.

[RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: mariadb-publish-logs-to-cloudwatch-logs

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `logTypes` | MariaDB DB 인스턴스가 CloudWatch Logs에 게시하도 | EnumList(최대 4개 항목) | `audit`, `error`, | `audit`, `error` |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 록 구성해야 하는 로그 유형의 목록입니다. DB 인스턴스가 목록에 지정된 유형의 로그를 게시하도록 구성되지 않은 경우, 제어는 FAILED 조사 결과를 생성합니다. | | general, slowquery | |

이 제어는 Amazon RDS for MariaDB DB 인스턴스가 다음 로그를 Amazon CloudWatch Logs에 게시하도록 구성되어 있는지 확인합니다. MariaDB DB 인스턴스가 로그를 CloudWatch Logs에 게시하도록 구성되지 않은 경우 제어가 실패합니다. 선택적으로 MariaDB DB 인스턴스가 게시하도록 구성해야 하는 로그 유형을 지정할 수 있습니다.

데이터베이스 로깅은 Amazon RDS for MariaDB DB 인스턴스에 대한 요청의 자세한 레코드를 제공합니다. 이러한 로그를 Amazon CloudWatch Logs에 게시하면 로그 관리를 중앙 집중화하고 로그 데이터에 대한 실시간 분석을 수행하는 데 도움이 됩니다. 또한 CloudWatch Logs는 보안, 액세스 및 가용성 검토 및 감사를 지원할 수 있는 내구성이 뛰어난 스토리지에 로그를 유지합니다. CloudWatch Logs를 사용하여 경보를 생성하고 지표를 볼 수도 있습니다.

문제 해결

Amazon RDS for MariaDB DB 인스턴스가 로그를 Amazon CloudWatch Logs에 게시하도록 구성하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 Amazon CloudWatch Logs에 MariaDB 로그 게시를 참조하세요.

[RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: AWS::RDS::DBProxy

AWS Config 규칙: rds-proxy-tls-encryption

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon RDS DB 프록시가 프록시와 기본 RDS DB 인스턴스 간의 모든 연결에 TLS를 요구하는지 여부를 확인합니다. 프록시가 프록시와 RDS DB 인스턴스 간의 모든 연결에 TLS를 요구하지 않는 경우 제어가 실패합니다.

Amazon RDS Proxy는 클라이언트 애플리케이션과 기본 RDS DB 인스턴스 사이에서 추가 보안 계층의 역할을 할 수 있습니다. 예를 들어 기본 DB 인스턴스가 이전 버전의 TLS를 지원하더라도 TLS 1.3을 사용하여 RDS 프록시에 연결할 수 있습니다. RDS Proxy를 사용하면 데이터베이스 애플리케이션에 강력한 인증 요구 사항을 적용할 수 있습니다.

문제 해결

Amazon RDS Proxy가 TLS를 요구하도록 설정을 변경하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 RDS 프록시 수정을 참조하세요.

[RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: rds-mariadb-instance-encrypted-in-transit

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon RDS for MariaDB DB 인스턴스에 대한 연결이 전송 중 암호화되는지 확인합니다. DB 인스턴스와 연결된 DB 파라미터 그룹이 동기화되지 않거나 파라미터 그룹의 `require_secure_transport` 파라미터가 `ON`으로 설정된 경우 제어가 실패합니다.

> **Note**
>
> 이 제어는 MariaDB 버전 10.5보다 낮은 버전을 사용하는 Amazon RDS DB 인스턴스를 평가하지 않습니다. `require_secure_transport` 파라미터는 MariaDB 버전 10.5 이상에서만 지원됩니다.

전송 중 데이터는 DB 클러스터의 노드 사이 또는 DB 클러스터와 클라이언트 애플리케이션 사이와 같이 한 위치에서 다른 위치로 이동하는 데이터를 나타냅니다. 데이터는 인터넷을 통해 또는 프라이빗 네

트워크 내에서 이동할 수 있습니다. 전송 중 데이터를 암호화하면 권한이 없는 사용자가 네트워크 트래픽을 도청할 위험이 줄어듭니다.

문제 해결

Amazon RDS for MariaDB DB 인스턴스에 연결하기 위해 SSL/TLS를 활성화하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 MariaDB DB 인스턴스에 대한 모든 연결에 SSL/TLS 요구를 참조하세요.

[RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: aurora-mysql-cluster-audit-logging

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Aurora MySQL DB 클러스터에 감사 로깅이 활성화되어 있는지 확인합니다. DB 클러스터와 연결된 DB 파라미터 그룹이 동기화되지 않거나 `server_audit_logging` 파라미터가 `1`로 설정되지 않았거나 `server_audit_events` 파라미터가 빈 값으로 설정된 경우 제어가 실패합니다.

데이터베이스 로그는 보안 및 액세스 감사에 도움이 되며 가용성 문제를 진단하는 데 도움이 될 수 있습니다. 감사 로그는 로그인 시도, 데이터 수정, 스키마 변경 및 보안 및 규정 준수를 위해 감사할 수 있는 기타 이벤트를 포함한 데이터베이스 활동 기록을 캡처합니다.

문제 해결

Amazon Aurora MySQL DB 클러스터에서 로깅을 활성화하는 방법에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon CloudWatch Logs에 Amazon Aurora MySQL 로그 게시를 참조하세요.

[RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::RDS::DBInstance`

AWS Config 규칙: rds-instance-subnet-igw-check

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon RDS DB 인스턴스가 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포되었는지 확인합니다. RDS DB 인스턴스가 인터넷 게이트웨이에 대한 경로가 있고 대상이 `0.0.0.0/0` 또는 `::/0`으로 설정된 서브넷에 배포된 경우 제어가 실패합니다.

Amazon RDS 리소스를 프라이빗 서브넷에 프로비저닝하면 RDS 리소스가 퍼블릭 인터넷에서 인바운드 트래픽을 수신하지 못하게 하여 RDS DB 인스턴스에 대한 의도하지 않은 액세스를 방지할 수 있습니다. RDS 리소스가 인터넷에 개방된 퍼블릭 서브넷에 프로비저닝되면 데이터 유출과 같은 위험에 취약할 수 있습니다.

문제 해결

Amazon RDS DB 인스턴스를 프라이빗 서브넷에 프로비저닝하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 VPC에서 DB 인스턴스를 사용한 작업을 참조하세요.

[RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: rds-pgsql-cluster-copy-tags-to-snapshot-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS for PostgreSQL DB 클러스터가 DB 클러스터의 스냅샷이 생성될 때 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다. RDS for PostgreSQL DB 클러스터에 대해 `CopyTagsToSnapshot` 파라미터가 `false`로 설정된 경우 제어가 실패합니다.

DB 스냅샷에 태그를 복사하면 백업 리소스 간에 적절한 리소스 추적, 거버넌스, 비용 할당을 유지하는 데 도움이 됩니다. 그러면 활성 데이터베이스와 스냅샷 모두에서 일관된 리소스 식별, 액세스 제어, 규정 준수 모니터링이 가능합니다. 스냅샷에 적절한 태그를 지정하면 백업 리소스가 소스 데이터베이스와 동일한 메타데이터를 상속하므로 보안 작업을 개선합니다.

문제 해결

Amazon RDS for PostgreSQL DB 클러스터가 자동으로 DB 스냅샷에 태그를 복사하도록 구성하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하세요.

[RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: rds-mysql-cluster-copy-tags-to-snapshot-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon RDS for MySQL DB 클러스터가 DB 클러스터의 스냅샷이 생성될 때 모든 태그를 스냅샷에 복사하도록 구성되어 있는지 확인합니다. RDS for MySQL DB 클러스터에 대해 `CopyTagsToSnapshot` 파라미터가 `false`로 설정된 경우 제어가 실패합니다.

DB 스냅샷에 태그를 복사하면 백업 리소스 간에 적절한 리소스 추적, 거버넌스, 비용 할당을 유지하는 데 도움이 됩니다. 그러면 활성 데이터베이스와 스냅샷 모두에서 일관된 리소스 식별, 액세스 제어, 규정 준수 모니터링이 가능합니다. 스냅샷에 적절한 태그를 지정하면 백업 리소스가 소스 데이터베이스와 동일한 메타데이터를 상속하므로 보안 작업을 개선합니다.

문제 해결

Amazon RDS for MySQL DB 클러스터가 자동으로 DB 스냅샷에 태그를 복사하도록 구성하는 방법에 대한 자세한 내용은 Amazon Relational Database Service 사용 설명서의 Amazon RDS 리소스 태그 지정을 참조하세요.

[RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::RDS::DBCluster`

AWS Config 규칙: rds-cluster-backup-retention-check

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `minimumBackupRetentionPeriod` | 컨트롤이 확인할 최소 백업 보존 기간 | Integer | 7~35 | 7 | |

이 제어는 RDS DB 클러스터에 최소 백업 보존 기간이 있는지 확인합니다. 백업 보존 기간이 지정된 파라미터 값보다 작으면 제어가 실패합니다. 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 7일을 사용합니다.

이 제어는 RDS DB 클러스터에 최소 백업 보존 기간이 있는지 확인합니다. 백업 보존 기간이 지정된 파라미터 값보다 작으면 제어가 실패합니다. 고객 파라미터 값을 제공하지 않는 한 Security Hub는 기본값인 7일을 사용합니다. 이 제어는 Aurora DB 클러스터, DocumentDB 클러스터, NeptuneDB 클러스터 등을 포함한 모든 유형의 RDS DB 클러스터에 적용됩니다.

문제 해결

RDS DB 클러스터의 백업 보존 기간을 구성하려면 클러스터 설정을 수정하고 백업 보존 기간을 최소 7일(또는 제어 파라미터에 지정된 값)로 설정합니다. 자세한 지침은 Amazon Relational Database Service 사용 설명서의 백업 보존 기간을 참조하세요. Aurora DB 클러스터의 경우 Aurora용 Amazon Aurora 사용 설명서의 Aurora DB 클러스터 백업 및 복원 개요를 참조하세요. 다른 유형의 DB 클러스터(예: DocumentDB 클러스터)는 해당 서비스 사용 설명서에서 클러스터의 백업 보존 기간을 업데이트하는 방법을 참조하세요.

[RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 높음

리소스 유형: `AWS::RDS::GlobalCluster`

AWS Config 규칙: rds-global-cluster-aurora-mysql-supported-version

스케줄 유형: 변경이 트리거됨

파라미터:

- `minSupportedEngineVersion`: `8.0.mysql_aurora.3.08.0`(사용자 지정할 수 없음)
- `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`(사용자 지정할 수 없음)

이 제어는 Amazon Aurora MySQL 글로벌 클러스터가 지원되는 최소 엔진 버전에서 실행 중인지 확인합니다. Aurora MySQL 글로벌 클러스터 엔진 버전이 지정된 최소 지원 버전보다 낮고 장기 지원 버전 파라미터에 나열되지 않으면 제어가 실패합니다.

지원되는 엔진 버전에서 Aurora MySQL 글로벌 데이터베이스를 실행하면 최신 보안 패치, 버그 수정 및 성능 개선 사항에 액세스할 수 있습니다. Aurora MySQL 마이너 버전은 end-of-standard-support을 정의했으며, 그 이후에는 더 이상 중요한 패치를 받지 않습니다. 지원되지 않는 버전을 실행하면 글로벌 데이터베이스가 보안 취약성에 노출되어 Amazon RDS 추가 지원 요금이 발생할 수 있습니다. Aurora MySQL은 장기 지원(LTS) 버전이 후속 비LTS 버전보다 더 오래 지원되는 비연속 지원 수명 주기를 따르므로이 제어는 여전히 표준 지원 중인 LTS 버전도 확인합니다. 자세한 내용은 Aurora MySQL용 Amazon Aurora 릴리스 정보의 Amazon Aurora MySQL 릴리스 일정을 참조하세요 MySQL.

문제 해결

Aurora MySQL 글로벌 데이터베이스를 지원되는 엔진 버전으로 업그레이드하는 방법에 대한 자세한 내용은 Amazon Aurora 사용 설명서의 Amazon Aurora 글로벌 데이터베이스 업그레이드 및 엔진 버전을 수정하여 Aurora MySQL 업그레이드를 참조하세요.

## Amazon Redshift에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Redshift 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-cluster-public-access-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터가 퍼블릭 액세스가 가능한지 여부를 확인합니다. 이는 클러스터 구성 항목의 `PubliclyAccessible` 필드를 평가합니다.

Amazon Redshift 클러스터 구성의 `PubliclyAccessible` 속성은 클러스터에 공개적으로 액세스할 수 있는지 여부를 나타냅니다. 클러스터가 `true`로 설정된 `PubliclyAccessible`로 구성된 경우, 이는 퍼블릭 IP 주소로 확인되는 공개적으로 확인 가능한 DNS 이름이 있는 인터넷 연결 인스턴스입니다.

클러스터에 퍼블릭 액세스가 불가능한 경우, 이는 프라이빗 IP 주소로 확인되는 DNS 이름을 가진 내부 인스턴스입니다. 클러스터를 공개적으로 액세스할 수 있도록 하려는 경우가 아니라면 클러스터를 `true`로 설정된 `PubliclyAccessible`로 구성해서는 안 됩니다.

문제 해결

Amazon Redshift 클러스터를 업데이트하여 퍼블릭 액세스를 비활성화하려면 Amazon Redshift 관리 안내서의 클러스터 수정을 참조하세요. 퍼블릭 액세스 가능을 아니오로 설정합니다.

[Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster` `AWS::Redshift::ClusterParameterGroup`

AWS Config 규칙: redshift-require-tls-ssl

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 전송 중 암호화를 사용하기 위해 Amazon Redshift 클러스터에 대한 연결이 필요한지 여부를 확인합니다. Amazon Redshift 클러스터 파라미터 `require_SSL`가 `True`로 설정되지 않은 경우, 확인이 실패합니다.

TLS를 사용하면 잠재적인 공격자가 중간자 또는 유사한 공격을 사용하여 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다. TLS를 통한 암호화된 연결만 허용되어야 합니다. 전송 중 데이터를 암호화하면 성능에 영향을 미칠 수 있습니다. 이 기능으로 애플리케이션을 테스트하여 성능 프로필과 TLS의 영향을 이해해야 합니다.

문제 해결

암호화를 요구하도록 Amazon Redshift 파라미터 그룹을 업데이트하려면 Amazon Redshift 관리 안내서의 파라미터 그룹 수정을 참조하세요. `require_ssl`를 true로 설정합니다.

[Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 복구 > 복원력 > 백업 활성화

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-backup-enabled

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 | |
|---|---|---|---|---|---|
| `MinRetentionPeriod` | 최소 스냅샷 보존 기간(일 수) | Integer | `7~35` | 7 | |

이 제어는 Amazon Redshift 클러스터에 자동 스냅샷이 활성화되어 있고 보존 기간이 지정된 기간 이상인지 확인합니다. 클러스터에서 자동 스냅샷을 사용할 수 없거나 보존 기간이 지정된 기간보다 짧으면 제어가 실패합니다. 스냅샷 보존 기간 동안 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 7일을 사용합니다.

백업을 통해 보안 사고로부터 더 빠르게 복구할 수 있습니다. 이는 시스템의 복원력을 강화합니다. Amazon Redshift는 기본적으로 주기적인 스냅샷을 찍습니다. 이 제어는 자동 스냅샷이 활성화되고 7일 이상 보관되는지 확인합니다. Amazon Redshift 자동 스냅샷에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 자동 스냅샷을 참조하세요.

문제 해결

Amazon Redshift 클러스터의 스냅샷 보존 기간을 업데이트하려면 Amazon Redshift 관리 안내서의 클러스터 수정을 참조하세요. 백업의 경우, 스냅샷 보존 값을 7 이상으로 설정합니다.

[Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config규칙: `redshift-cluster-audit-logging-enabled` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터에 감사 로깅이 활성화되어 있는지 여부를 확인합니다.

Amazon Redshift 감사 로깅은 클러스터 내 연결 및 사용자 작업에 대한 추가 정보를 제공합니다. 이 데이터는 Amazon S3에 저장 및 보호될 수 있으며 보안 감사 및 조사에 유용할 수 있습니다. 자세한 내용은 Amazon Redshift 관리 안내서의 데이터베이스 감사 로깅을 참조하세요.

문제 해결

Amazon Redshift 클러스터에 대한 감사 로깅을 구성하려면 Amazon Redshift 관리 안내서의 콘솔을 사용하여 감사 구성을 참조하세요.

[Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.

관련 요구 사항: 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)

범주: 식별 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-cluster-maintenancesettings-check

스케줄 유형: 변경이 트리거됨

파라미터:

- `allowVersionUpgrade = true`(사용자 지정할 수 없음)

이 제어는 Amazon Redshift 클러스터에 자동 메이저 버전 업그레이드가 활성화되어 있는지 여부를 확인합니다.

자동 메이저 버전 업그레이드를 활성화하면 유지 관리 기간 중에 Amazon Redshift 클러스터에 대한 최신 메이저 버전 업데이트가 설치됩니다. 이러한 업데이트에는 보안 패치 및 버그 수정이 포함될 수 있습니다. 패치 설치를 최신 상태로 유지하는 것은 시스템 보안의 중요한 단계입니다.

문제 해결

에서이 문제를 해결하려면 Amazon Redshift `modify-cluster` 명령을 AWS CLI사용하고 `--allow-version-upgrade` 속성을 설정합니다. *`clustername`*는 Amazon Redshift 클러스터의 이름입니다.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

[Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성 > API 프라이빗 액세스

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-enhanced-vpc-routing-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터에 `EnhancedVpcRouting`가 활성화되었는지 여부를 확인합니다.

향상된 VPC 라우팅은 클러스터와 데이터 저장소 사이의 모든 `COPY` 및 `UNLOAD` 트래픽이 VPC를 통과하도록 강제합니다. 그런 다음 보안 그룹 및 네트워크 액세스 제어 목록과 같은 VPC 기능을 사용하여 네트워크 트래픽을 보호할 수 있습니다. 또한 VPC 흐름 로그를 사용하여 네트워크 트래픽을 모니터링할 수 있습니다.

문제 해결

자세한 수정 지침은 Amazon Redshift 관리 안내서의 향상된 VPC 라우팅 활성화를 참조하세요.

[Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-default-admin-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터가 관리자 사용자 이름을 기본값에서 변경했는지 여부를 확인합니다. Redshift 클러스터의 관리자 사용자 이름이 `awsuser`로 설정된 경우, 이 제어가 실패합니다.

Redshift 클러스터를 만들 때는 기본 관리자 사용자 이름을 고유한 값으로 변경해야 합니다. 기본 사용자 이름은 공개되어 있으므로 구성 시 변경해야 합니다. 기본 사용자 이름을 변경하면 의도하지 않은 액세스의 위험이 줄어듭니다.

문제 해결

Amazon Redshift 클러스터가 생성된 후에는 해당 클러스터의 관리자 사용자 이름을 변경할 수 없습니다. 기본이 아닌 사용자 이름으로 새로운 클러스터를 생성하려면 Amazon Redshift 시작 안내서의 1단계: 샘플 Amazon Redshift 클러스터 생성을 참조하세요.

[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-cluster-kms-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터가 저장 시 암호화되었는지 확인합니다. Redshift 클러스터가 저장 시 암호화되지 않거나 암호화 키가 규칙 파라미터에 제공된 키와 다른 경우, 제어가 실패합니다.

Amazon Redshift에서는 클러스터의 데이터베이스 암호화를 통해 저장된 데이터를 보호할 수 있습니다. 클러스터에서 암호화를 활성화하면 해당 클러스터와 스냅샷의 데이터 블록 및 시스템 메타데이터

가 암호화됩니다. 저장 데이터 암호화는 데이터에 액세스 관리 계층을 추가하므로 권장되는 모범 사례입니다. 저장된 Redshift 클러스터를 암호화하면 권한이 없는 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다.

문제 해결

KMS 암호화를 사용하도록 Redshift 클러스터를 수정하려면 Amazon Redshift 관리 안내서의 클러스터 암호화 변경을 참조하세요.

[Redshift.11] Redshift 클러스터에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Redshift::Cluster`

AWS Config규칙: `tagged-redshift-cluster` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon Redshift 클러스터에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 클러스터에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 클러스터에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는

데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Redshift 클러스터에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift에서 리소스 태그 지정을 참조하세요.

[Redshift.12] Redshift 이벤트 알림 구독에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Redshift::EventSubscription`

AWS Config규칙: `tagged-redshift-eventsubscription` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon Redshift 클러스터 스냅샷에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 클러스터 스냅샷에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 클러스터 스냅샷에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Redshift 이벤트 알림 구독에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift에서 리소스 태그 지정을 참조하세요.

[Redshift.13] Redshift 클러스터 스냅샷에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Redshift::ClusterSnapshot`

AWS Config규칙: `tagged-redshift-clustersnapshot` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon Redshift 클러스터 스냅샷에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 클러스터 스냅샷에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 클러스터 스냅샷에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Redshift 클러스터 스냅샷에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift에서 리소스 태그 지정을 참조하세요.

[Redshift.14] Redshift 클러스터 서브넷 그룹에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Redshift::ClusterSubnetGroup`

AWS Config규칙: `tagged-redshift-clustersubnetgroup` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 Amazon Redshift 클러스터 서브넷 그룹에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 클러스터 서브넷 그룹에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 클러스터 서브넷에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Redshift 클러스터 서브넷 그룹에 태그를 추가하려면 Amazon Redshift 관리 안내서의 Amazon Redshift에서 리소스 태그 지정을 참조하세요.

[Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.

관련 요구 사항: PCI DSS v4.0.1/1.3.1

범주: 보호 > 보안 네트워크 구성 > 보안 그룹 구성

심각도: 높음

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-unrestricted-port-access

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Redshift 클러스터와 연결된 보안 그룹에 인터넷(0.0.0.0/0 또는 ::/0)에서 클러스터 포트에 대한 액세스를 허용하는 수신 규칙이 있는지 확인합니다. 보안 그룹 수신 규칙이 인터넷에서 클러스터 포트에 대한 액세스를 허용하는 경우, 제어가 실패합니다.

Redshift 클러스터 포트에 대한 무제한 인바운드 액세스(접미사가 /0인 IP 주소)를 허용하면 무단 액세스 또는 보안 인시던트가 발생할 수 있습니다. 보안 그룹을 생성하고 인바운드 규칙을 구성할 때 최소 권한 액세스의 보안 주체를 적용하는 것이 좋습니다.

문제 해결

Redshift 클러스터 포트의 수신을 제한된 오리진으로 제한하려면 Amazon VPC 사용 설명서의 보안 그룹 규칙 작업을 참조하세요. 포트 범위가 Redshift 클러스터 포트와 일치하고 IP 포트 범위가 0.0.0.0/0인 규칙을 업데이트합니다.

[Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Redshift::ClusterSubnetGroup`

AWS Config 규칙: redshift-cluster-subnet-group-multi-az

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터 서브넷 그룹에 2개 이상의 다른 가용 영역(AZ)의 서브넷이 있는지 확인합니다. 클러스터 서브넷 그룹에 적어도 2개 이상의 다른 AZ의 서브넷이 없으면 제어가 실패합니다.

여러 AZ에 서브넷을 구성하면 장애 이벤트가 발생하더라도 Redshift 데이터 웨어하우스가 계속 작동할 수 있습니다.

문제 해결

여러 AZ에 걸쳐 있도록 Redshift 클러스터 서브넷 그룹을 수정하려면 Amazon Redshift 관리 안내서의 클러스터 서브넷 그룹 수정을 참조하세요.

[Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Redshift::ClusterParameterGroup`

AWS Config 규칙: redshift-cluster-parameter-group-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon Redshift 클러스터 파라미터 그룹에 파라미터 `requiredKeyTags`에 지정된 태그가 있는지 확인합니다. 파라미터 그룹에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 파라미터 그룹에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Redshift 클러스터 파라미터 그룹에 태그를 추가하는 방법에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 Amazon Redshift에서 리소스 태그 지정을 참조하세요.

[Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::Redshift::Cluster`

AWS Config 규칙: redshift-cluster-multi-az-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Redshift 클러스터에 대해 다중 가용 영역(다중 AZ) 배포가 활성화되어 있는지 확인합니다. Amazon Redshift 클러스터에 다중 AZ 배포가 활성화되지 않은 경우 제어가 실패합니다.

Amazon Redshift는 프로비저닝된 클러스터에 다중 가용 영역(다중 AZ) 배포를 지원합니다. 클러스터에 대해 다중 AZ 배포를 활성화하면 Amazon Redshift 데이터 웨어하우스는 한 가용 영역(AZ)에서 예기치 않은 이벤트가 발생하는 장애 시나리오에서 계속 작동할 수 있습니다. 다중 AZ 배포는 2개 이의 AZ에 컴퓨팅 리소스를 배포하며, 이러한 컴퓨팅 리소스는 단일 엔드포인트를 통해 액세스할 수 있습니다. 전체 AZ에 장애가 발생하는 경우 두 번째 AZ의 나머지 컴퓨팅 리소스를 계속해서 워크로드를 처리하는 데 사용할 수 있습니다. 기존 단일 AZ 데이터 웨어하우스를 다중 AZ 데이터 웨어하우스로 변환할 수 있습니다. 그러면 두 번째 AZ에 추가 컴퓨팅 리소스가 프로비저닝됩니다.

문제 해결

Amazon Redshift 클러스터에 대해 다중 AZ 배포를 구성하는 방법에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 단일 AZ 데이터 웨어하우스를 다중 AZ 데이터 웨어하우스로 변환을 참조하세요.

## Amazon Redshift Serverless에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Redshift Serverless 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 높음

리소스 유형: `AWS::RedshiftServerless::Workgroup`

AWS Config 규칙: redshift-serverless-workgroup-routes-within-vpc

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Redshift Serverless 작업 그룹에 대해 향상된 VPC 라우팅이 활성화되어 있는지 확인합니다. 작업 그룹에 대해 향상된 VPC 라우팅이 비활성화된 경우 제어가 실패합니다.

Amazon Redshift Serverless 작업 그룹에 대해 향상된 VPC 라우팅이 비활성화된 경우 Amazon Redshift는 AWS네트워크 내의 다른 서비스로 트래픽을 포함하여 인터넷을 통해 트래픽을 라우팅합니다. 작업 그룹에 대해 향상된 VPC 라우팅을 활성화하면 Amazon Redshift는 클러스터와 데이터 리포지토리 사이의 `COPY` 및 `UNLOAD` 트래픽이 모두 Amazon VPC 서비스를 기반으로 하는 가상 프라이빗 클라우드(VPC)를 통과하도록 강제합니다. 향상된 VPC 라우팅을 사용하여 Amazon Redshift 클러스터와 다른 리소스 간의 데이터 흐름을 제어할 수 있습니다. 여기에는 VPC 보안 그룹 및 엔드포인트 정책, 네트워크 액세스 제어 목록(ACL), 도메인 이름 시스템(DNS) 서버와 같은 기능이 포함됩니다. VPC 흐름 로그를 사용하여 `COPY` 및 `UNLOAD` 트래픽을 모니터링할 수도 있습니다.

문제 해결

향상된 VPC 라우팅 및 작업 그룹에 대해 이 기능을 활성화하는 방법에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 Redshift 향상된 VPC 라우팅을 사용하여 네트워크 트래픽 제어를 참조하세요.

[RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RedshiftServerless::Workgroup`

AWS Config 규칙: redshift-serverless-workgroup-encrypted-in-transit

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Redshift Serverless 작업 그룹에 대한 연결이 전송 중 데이터를 암호화해야 하는지 확인합니다. 작업 그룹의 `require_ssl` 구성 파라미터가 `false`로 설정된 경우 제어가 실패합니다.

Amazon Redshift Serverless 작업 그룹은 RPU, VPC 서브넷 그룹, 보안 그룹과 같은 컴퓨팅 리소스를 그룹화하는 컴퓨팅 리소스 모음입니다. 작업 그룹의 속성에는 네트워크 및 보안 설정이 포함됩니다. 이러한 설정은 작업 그룹에 대한 연결이 SSL을 사용하여 전송 중 데이터를 암호화해야 하는지 여부를 지정합니다.

문제 해결

SSL 연결을 요구하도록 Amazon Redshift Serverless 작업 그룹의 설정을 업데이트하는 방법에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 Amazon Redshift Serverless에 연결을 참조하세요.

[RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::RedshiftServerless::Workgroup`

AWS Config 규칙: redshift-serverless-workgroup-no-public-access

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Redshift Serverless 작업 그룹에 대해 퍼블릭 액세스가 비활성화되었는지 확인합니다. 이를 위해 Redshift Serverless 작업 그룹의 `publiclyAccessible` 속성을 평가합니다. 작업 그룹에 대해 퍼블릭 액세스가 활성화된 경우(`true`) 제어가 실패합니다.

Amazon Redshift Serverless 작업 그룹에 대한 퍼블릭 액세스(`publiclyAccessible`) 설정은 퍼블릭 네트워크에서 작업 그룹에 액세스할 수 있는지 여부를 지정합니다. 작업 그룹에 대해 퍼블릭 액세스가 활성화된 경우(`true`) Amazon Redshift는 VPC 외부에서 작업 그룹에 공개적으로 액세스할 수 있는 탄력적 IP 주소를 생성합니다. 작업 그룹에 공개적으로 액세스할 수 없도록 하려면 해당 작업 그룹에 대한 퍼블릭 액세스를 비활성화합니다.

문제 해결

Amazon Redshift Serverless 작업 그룹의 퍼블릭 액세스 설정을 변경하는 방법에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 작업 그룹 속성 보기를 참조하세요.

[RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::RedshiftServerless::Namespace`

AWS Config 규칙: redshift-serverless-namespace-cmk-encryption

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `kmsKeyArns` | 평가에 AWS KMS keys포함할의 Amazon 리소스 이름(ARNs) 목록입니다. Redshift Serverless 네임스페이스가 목록의 KMS 키로 암호화되지 않은 경우, 제어가 `FAILED` 조사 결과를 생성합니다. | StringList(최대 3개 항목) | 기존 KMS 키의 ARN 1~3개. 예를 들어 `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab` 입니다. | 기본값 없음 |

이 제어는 Amazon Redshift Serverless 네임스페이스가 고객 관리형 AWS KMS key로 저장 시 암호화되는지 확인합니다. Redshift Serverless 네임스페이스가 고객 관리형 KMS 키로 암호화되지 않는 경우 제어가 실패합니다. 선택적으로 평가에 포함할 제어에 대한 KMS 키 목록을 지정할 수 있습니다.

Amazon Redshift Serverless에서 네임스페이스는 데이터베이스 객체에 대한 논리적 컨테이너를 정의합니다. 이 제어는 네임스페이스의 암호화 설정이 네임스페이스의 데이터 암호화를 위해 관리형 KMS 키 AWS KMS key대신 고객 AWS관리형를 지정하는지 여부를 주기적으로 확인합니다. 고객 관리형 KMS 키를 사용하면 고객이 키를 완전히 제어할 수 있습니다. 여기에는 키 정책 정의 및 유지 관리, 권한 부여 관리, 암호화 자료 교체, 태그 할당, 별칭 생성, 키 활성화 및 비활성화가 포함됩니다.

문제 해결

Amazon Redshift Serverless 네임스페이스의 암호화 설정 업데이트 및 고객 관리형 지정에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 네임스페이스에 AWS KMS key대한 변경을 AWS KMS key 참조하세요.

[RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다

범주: 식별 > 리소스 구성

심각도: 중간

리소스 유형: `AWS::RedshiftServerless::Namespace`

AWS Config 규칙: redshift-serverless-default-admin-check

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Redshift Serverless 네임스페이스의 관리자 사용자 이름이 기본 관리자 사용자 이름인 `admin`인지 확인합니다. Redshift Serverless 네임스페이스의 관리자 사용자 이름이 `admin`인 경우 제어가 실패합니다.

Amazon Redshift Serverless 네임스페이스를 생성할 때 네임스페이스의 사용자 지정 관리자 사용자 이름을 지정해야 합니다. 기본 관리자 사용자 이름은 공개 지식입니다. 사용자 지정 관리자 사용자 이름을 지정하면 예를 들어 네임스페이스에 대한 무차별 대입 공격의 위험 또는 효과를 완화하는 데 도움이 될 수 있습니다.

문제 해결

Amazon Redshift Serverless 콘솔 또는 API를 사용하여 Amazon Redshift Serverless 네임스페이스의 관리자 사용자 이름을 변경할 수 있습니다. 콘솔을 사용하여 변경하려면 네임스페이스 구성을 선택한 다음 작업 메뉴에서 관리자 자격 증명 편집을 선택합니다. 프로그래밍 방식으로 변경하려면 UpdateNamespace 작업을 사용하거나를 사용하는 경우 update-namespace 명령을 AWS CLI실행합니다. 관리자 사용자 이름을 변경하는 경우 동시에 관리자 암호도 변경해야 합니다.

[RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::RedshiftServerless::Namespace`

AWS Config 규칙: redshift-serverless-publish-logs-to-cloudwatch

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon Redshift Serverless 네임스페이스가 연결 및 사용자 로그를 Amazon CloudWatch Logs로 내보내도록 구성되어 있는지 확인합니다. Redshift Serverless 네임스페이스가 로그를 CloudWatch Logs로 내보내도록 구성되지 않은 경우 제어가 실패합니다.

연결 로그(`connectionlog`) 및 사용자 로그(`userlog`) 데이터를 Amazon CloudWatch Logs의 로그 그룹으로 내보내도록 Amazon Redshift Serverless를 구성하면 보안, 액세스 및 가용성 검토 및 감사를 지원할 수 있는 내구성이 뛰어난 스토리지에 로그 레코드를 수집하고 저장할 수 있습니다. CloudWatch Logs를 사용하면 로그 데이터에 대한 실시간 분석을 수행하고 CloudWatch를 사용하여 경보를 생성하고 지표를 확인할 수도 있습니다.

문제 해결

Amazon Redshift Serverless 네임스페이스의 로그 데이터를 Amazon CloudWatch Logs로 내보내려면 네임스페이스에 대한 감사 로깅 구성 설정에서 해당 로그를 내보내도록 선택해야 합니다. 이러한 설정을 업데이트하는 방법에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 보안 및 암호화 편집을 참조하세요.

## Route 53에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Route 53 서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::Route53::HealthCheck`

AWS Config규칙:`tagged-route53-healthcheck` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon Route 53 상태 확인에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 상태 확인에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우 제어는 태그 키의 존재만 확인하고 상태 확인에 키로 태그가 지정되지 않은 경우, 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Route 53 상태 확인에 태그를 추가하려면 Amazon Route 53 개발자 안내서의 상태 확인 이름 지정 및 태그 지정을 참조하세요.

[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Route53::HostedZone`

AWS Config 규칙: `route53-query-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon Route 53 퍼블릭 호스팅 영역에 대해 DNS 쿼리 로깅이 활성화되어 있는지 확인합니다. Route 53 퍼블릭 호스팅 영역에 대해 DNS 쿼리 로깅을 활성화하지 않으면 제어가 실패합니다.

Route 53 호스팅 영역에 대한 DNS 쿼리를 로깅하면 DNS 보안 및 규정 준수 요구 사항을 해결하고 가시성을 확보할 수 있습니다. 로그에는 쿼리된 도메인 또는 하위 도메인, 쿼리 날짜 및 시간, DNS 레코드 유형(예: A 또는 AAAA), DNS 응답 코드(예제: `NoError` 또는 `ServFail`) 등의 정보가 포함됩니다. DNS 쿼리 로깅이 활성화되면 Route 53은 로그 파일을 Amazon CloudWatch Logs에 게시합니다.

문제 해결

Route 53 퍼블릭 호스팅 영역에 대한 DNS 쿼리를 로깅하려면 Amazon Route 53 개발자 안내서의 DNS 쿼리에 대한 로깅 구성을 참조하세요.

## Amazon S3에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon Simple Storage Service(Amazon S3) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.1.4, CIS AWS 파운데이션 벤치마크 v3.0.0/2.1.4, CIS AWS 파운데이션 벤치마크 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-77 NIST.800-53.r5 SC-7,

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: s3-account-level-public-access-blocks-periodic

스케줄 유형: 주기적

파라미터:

- `ignorePublicAcls`: `true`(사용자 지정할 수 없음)
- `blockPublicPolicy`: `true`(사용자 지정할 수 없음)
- `blockPublicAcls`: `true`(사용자 지정할 수 없음)
- `restrictPublicBuckets`: `true`(사용자 지정할 수 없음)

이 제어는 이전 Amazon S3 Block Public Access 설정이 S3 법용 버킷에 대한 계정 수준에서 구성되었는지 확인합니다. 퍼블릭 액세스 차단 설정 중 하나 이상이 `false`로 설정된 경우, 제어가 실패합니다.

설정 중 하나라도 `false`으로 설정되어 있거나 설정이 구성되지 않은 경우, 제어가 실패합니다.

Amazon S3 퍼블릭 액세스 블록은 객체에 퍼블릭 액세스가 없도록 전체 AWS 계정 또는 개별 S3 버킷 수준에서 제어를 제공하도록 설계되었습니다. 액세스 제어 목록(ACL), 버킷 정책 또는 둘 다를 통해 버킷 및 객체에 퍼블릭 액세스 권한이 부여됩니다.

S3 버킷에 대한 퍼블릭 액세스를 가능하도록 하려는 경우가 아니면 계정 수준의 Amazon S3 Block Public Access 기능을 구성해야 합니다.

자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 Block Public Access 사용을 참조하세요.

문제 해결

에 대해 Amazon S3 퍼블릭 액세스 차단을 활성화하려면 Amazon Simple Storage Service 사용 설명서의 계정에 대한 퍼블릭 액세스 차단 설정 구성을 AWS 계정참조하세요. https://docs.aws.amazon.com/AmazonS3/latest/userguide/configuring-block-public-access-account.html

[S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-public-read-prohibited

스케줄 유형: 주기적이며 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷이 퍼블릭 읽기 액세스를 허용하는지 여부를 확인합니다. 퍼블릭 액세스 차단 설정, 버킷 정책 및 버킷 ACL(액세스 제어 목록)을 평가합니다. 버킷이 퍼블릭 읽기 액세스를 허용하면 제어가 실패합니다.

> **Note**
>
> S3 버킷에 버킷 정책이 있는 경우 이 제어는 와일드카드 문자 또는 변수를 사용하는 정책 조건을 평가하지 않습니다. `PASSED` 조사 결과를 생성하려면 버킷 정책의 조건이 고정 값, 즉 와일드카드 문자 또는 정책 변수를 포함하지 않는 값만 사용해야 합니다. 정책 변수에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 변수 및 태그를 참조하세요.

일부 사용 사례에서는 인터넷의 모든 사용자가 S3 버킷에서 읽을 수 있어야 합니다. 그러나 이러한 상황은 드뭅니다. 데이터의 무결성과 보안을 보장하기 위해 S3 버킷은 공개적으로 읽을 수 없습니다.

문제 해결

Amazon S3 버킷에 대한 퍼블릭 읽기 액세스를 차단하려면 Amazon 심플 스토리지 서비스 사용 설명서의 S3 버킷에 대한 퍼블릭 액세스 차단 설정 구성을 참조하세요.

[S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 심각

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-public-write-prohibited

스케줄 유형: 주기적이며 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷이 퍼블릭 쓰기 액세스를 허용하는지 여부를 확인합니다. 퍼블릭 액세스 차단 설정, 버킷 정책 및 버킷 ACL(액세스 제어 목록)을 평가합니다. 버킷이 퍼블릭 쓰기 액세스를 허용하면 제어가 실패합니다.

> **Note**
>
> S3 버킷에 버킷 정책이 있는 경우 이 제어는 와일드카드 문자 또는 변수를 사용하는 정책 조건을 평가하지 않습니다. `PASSED` 조사 결과를 생성하려면 버킷 정책의 조건이 고정 값, 즉 와일드카드 문자 또는 정책 변수를 포함하지 않는 값만 사용해야 합니다. 정책 변수에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 변수 및 태그를 참조하세요.

일부 사용 사례에서는 인터넷의 모든 사용자가 S3 버킷에 쓸 수 있어야 합니다. 그러나 이러한 상황은 드뭅니다. 데이터의 무결성과 보안을 보장하기 위해 S3 버킷은 공개적으로 쓸 수 없습니다.

문제 해결

Amazon S3 버킷에 대한 퍼블릭 쓰기 액세스를 차단하려면 Amazon 심플 스토리지 서비스 사용 설명서의 S3 버킷에 대한 퍼블릭 액세스 차단 설정 구성을 참조하세요.

[S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.1.1, CIS AWS 파운데이션 벤치마크 v3.0.0/2.1.1, CIS AWS 파운데이션 벤치마크 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, NIST.NIST.800-53.r5 SC-7 SC-53.r5 SC-23(33) NIST.800-53.r5 SC-8 SI-7 3.13.15

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-ssl-requests-only

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷에 TLS 사용 요청이 필요한 정책이 있는지 확인합니다. 버킷 정책에 TLS 사용 요청이 필요하지 않으면 제어가 실패합니다.

S3 버킷에는 S3 리소스 정책에 있는 HTTPS를 통한 데이터 전송만 허용하도록 모든 요청(`Action: S3:*`)을 요구하는 정책이 있어야 하며 조건 키 `aws:SecureTransport`으로 표시됩니다.

문제 해결

비보안 전송을 거부하도록 Amazon S3 버킷 정책을 업데이트하려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조하세요.

다음 정책에 있는 것과 유사한 정책 설명을 추가하세요. `amzn-s3-demo-bucket`를 수정하려는 버킷의 이름으로 바꿉니다.

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": "*"
        }
    ]
}
```

자세한 내용은 AWS Config 규칙 sS3bucket-ssl-requests-only. AWS 공식 지식 센터의 .

[S3.6] S3 범용 버킷 정책은 다른에 대한 액세스를 제한해야 합니다. AWS 계정

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2, NIST.800-171.r2 3.13.4

범주: 보호 > 보안 액세스 관리 > 민감한 API 작업 작업 제한

심각도: 높음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-blacklisted-actions-prohibited

스케줄 유형: 변경이 트리거됨

파라미터:

- `blacklistedactionpatterns`: `s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl`(사용자 지정할 수 없음)

이 제어는 S3 버킷 정책이 다른 AWS 계정 의 보안 주체가 S3 버킷의 리소스에 대해 거부된 작업을 수행하는 것을 방지하는지 확인합니다. 버킷 정책이 다른 AWS 계정의 보안 주체에 대해 이전 작업 중 하나 이상을 허용하는 경우, 제어가 실패합니다.

최소 권한 액세스를 구현하는 것은 보안 위험과 오류 또는 악의적 의도의 영향을 줄이는 데 필수적입니다. S3 버킷 정책에서 외부 계정으로부터의 액세스를 허용하는 경우, 내부자 위협이나 공격자에 의한 데이터 유출이 발생할 수 있습니다.

`blacklistedactionpatterns` 파라미터를 사용하면 S3 버킷의 규칙을 성공적으로 평가할 수 있습니다. 파라미터는 `blacklistedactionpatterns` 목록에 포함되지 않은 작업 패턴에 대해 외부 계정에 대한 액세스 권한을 부여합니다.

문제 해결

Amazon S3 버킷 정책을 업데이트하여 권한을 제거하려면 Amazon Simple Storage Service 사용 설명서의 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조하세요.

버킷 정책 편집 페이지의 정책 편집 텍스트 상자에서 다음 작업 중 하나를 수행하세요.

- 거부된 작업에 대한 다른 AWS 계정 액세스 권한을 다른 사람에게 부여하는 문을 삭제하세요.
- 명령문에서 허용된 거부된 작업을 제거합니다.

[S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-cross-region-replication-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷에 리전 간 복제가 활성화되어 있는지 확인합니다. 버킷에 교차 리전 복제가 활성화되어 있지 않으면 제어가 실패합니다.

복제는 동일하거나 다른의 버킷 간에 객체를 비동기식으로 자동 복사하는 것입니다 AWS 리전. 복제는 새롭게 생성된 객체와 객체 업데이트를 소스 버킷에서 대상 버킷으로 복사합니다. AWS 모범 사례에서

는 동일한 AWS 계정소유의 소스 및 대상 버킷에 대한 복제를 권장합니다. 가용성 외에도 다른 시스템 보안 강화 설정을 고려해야 합니다.

이 제어는 교차 리전 복제가 활성화되지 않은 복제 대상 버킷에 대한 `FAILED` 조사 결과를 생성합니다. 대상 버킷이 교차 리전 복제를 활성화할 필요가 없는 합법적인 이유가 있는 경우, 이 버킷에 대한 조사 결과를 숨길 수 있습니다.

문제 해결

S3 버킷에서 교차 리전 복제를 활성화하려면 Amazon Simple Storage Service 사용 설명서의 동일한 계정이 소유한 소스 및 대상 버킷에 대한 복제 구성을 참조하세요. 소스 버킷의 경우, 버킷의 모든 객체에 적용을 선택합니다.

[S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.1.4, CIS AWS 파운데이션 벤치마크 v3.0.02.1.4, CIS AWS 파운데이션 벤치마크 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( NIST.800-53.r5 SC-71

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 높음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-level-public-access-prohibited

스케줄 유형: 변경이 트리거됨

파라미터:

- `excludedPublicBuckets`(사용자 지정할 수 없음) - 알려진 허용된 퍼블릭 S3 버킷 이름을 쉼표로 구분한 목록입니다.

이 제어는 Amazon S3 범용 버킷이 버킷 수준에서 퍼블릭 액세스를 차단하는지 여부를 확인합니다. 다음 설정 중 하나가 `false`으로 설정된 경우, 이 제어가 실패합니다.

- `ignorePublicAcls`
- `blockPublicPolicy`

- `blockPublicAcls`
- `restrictPublicBuckets`

S3 버킷 수준에서의 퍼블릭 액세스 차단은 객체에 퍼블릭 액세스가 없도록 제어하는 기능을 제공합니다. 액세스 제어 목록(ACL), 버킷 정책 또는 둘 다를 통해 버킷 및 객체에 퍼블릭 액세스 권한이 부여됩니다.

S3 버킷에 대한 퍼블릭 액세스를 가능하도록 하려는 경우가 아니면 버킷 수준의 Amazon S3 Block Public Access 기능을 구성해야 합니다.

문제 해결

버킷 수준에서 퍼블릭 액세스를 제거하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 스토리지에 대한 퍼블릭 액세스 차단을 참조하세요.

[S3.9] S3 범용 버킷에는 서버 액세스 로깅이 활성화되어 있어야 합니다

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷에 대해 서버 액세스 로깅이 활성화되었는지 여부를 확인합니다. 서버 액세스 로깅이 활성화되어 있지 않으면 이 제어가 실패합니다. 로깅을 사용하도록 설정하면 Amazon S3는 소스 버킷에 대한 액세스 로그를 선택한 대상 버킷으로 전달합니다. 대상 버킷은 AWS 리전 소스 버킷과 동일한에 있어야 하며 기본 보존 기간이 구성되어 있지 않아야 합니다. 대상 로깅 버킷에는 서버 액세스 로깅을 활성화할 필요가 없으며 이 버킷에 대한 조사 결과를 표시하지 않아야 합니다.

서버 액세스 로깅은 버킷에 대한 요청에 대한 자세한 기록을 제공합니다. 서버 액세스 로그는 보안 및 액세스 감사에 도움이 될 수 있습니다. 자세한 내용은 Amazon S3 보안 모범 사례: Amazon S3 서버 액세스 로깅 활성화를 참조하세요.

문제 해결

Amazon S3 서버 액세스 로깅을 활성화하려면 Amazon S3 사용 설명서의 Amazon S3 서버 액세스 로깅 활성화를 참조하세요.

[S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-version-lifecycle-policy-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버전 관리된 버킷에 수명 주기 구성이 있는지 확인합니다. 버킷에 수명 주기 구성이 없는 경우, 제어가 실패합니다.

객체 수명 동안 Amazon S3가 수행할 작업을 정의하는 데 도움이 되므로 S3 버킷에 수명 주기 구성을 생성하는 것을 권장합니다.

> **Tip**
>
> 수명 주기 관리 없이 버전 관리를 활성화하면 스토리지가 무제한으로 증가하고 비용이 증가할 수 있습니다. 객체를 수정할 때마다 무기한 보관되는 새 버전이 생성됩니다. 비최신 버전을 더 저렴한 스토리지 클래스로 자동 전환하거나 정의된 보존 기간 후에 만료하도록 S3 수명 주기 규칙을 구성합니다.

문제 해결

Amazon S3 버킷에서 수명 주기를 구성하는 방법에 대한 자세한 내용은 Amazon SS3 사용 설명서의 S3 수명 주기에서 S3 버전 관리 사용, 버킷에서 수명 주기 구성 설정 및 객체의 수명 주기 관리를 참조하세요. Amazon S3

[S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-event-notifications-enabled

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `eventTypes` | 선호하는 S3 이벤트 유형 목록 | EnumList(최대 28개 항목) | `s3:IntelligentTiering, s3:LifecycleExpiration:*, s3:LifecycleExpiration:Delete, s3:LifecycleExpiration:DeleteMarkerC` | 기본값 없음 |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | | | reated, s3:Lifecycle Transition, 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 | |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | | | , s3:ObjectRestore:* , s3:ObjectRestore:Completed, s3:ObjectRestore:Delete, s3:ObjectRestore:Post, s3:ObjectTagging:* , s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, | |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | | | s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replication:OperationReplicatedAfterThreshold, s3:TestEvent | |

이 제어는 Amazon S3 범용 버킷에서 S3 이벤트 알림이 활성화되었는지 여부를 확인합니다. 버킷에서 S3 이벤트 알림을 활성화하지 않으면 제어가 실패합니다. eventTypes 파라미터에 사용자 지정 값을 제공하는 경우, 지정된 이벤트 유형에 대해 이벤트 알림이 활성화된 경우에만 제어가 통과합니다.

S3 이벤트 알림을 활성화하면 특정 이벤트가 발생할 때 S3 버킷에서 알림을 받게 됩니다. 예를 들어, 개체 생성, 개체 제거, 개체 복원에 대한 알림을 받을 수 있습니다. 이러한 알림은 무단 데이터 액세스로 이어질 수 있는 우발적이거나 의도적인 수정에 대해 관련 팀에 경고할 수 있습니다.

문제 해결

S3 버킷 및 객체 변경 감지에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 이벤트 알림을 참조하세요.

[S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 액세스 제어

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-acl-prohibited

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷이 액세스 제어 목록(ACL)을 통해 사용자 권한을 제공하는지 확인합니다. S3 버킷에 대한 사용자 액세스를 관리하도록 ACL이 구성된 경우, 제어가 실패합니다.

ACL은 IAM 이전의 레거시 액세스 제어 메커니즘입니다. ACLs 대신 S3 버킷 정책 또는 AWS Identity and Access Management (IAM) 정책을 사용하여 S3 버킷에 대한 액세스를 관리하는 것이 좋습니다.

문제 해결

이 제어를 통과하려면 S3 버킷에 대한 ACL을 비활성화해야 합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 객체 소유권 제어 및 버킷에 대해 ACL 비활성화를 참조하세요.

S3 버킷 정책을 생성하려면 Amazon S3 콘솔을 사용하여 버킷 정책 추가를 참조하세요. S3 버킷에 IAM 사용자 정책을 생성하려면 사용자 정책을 사용한 버킷 액세스 제어를 참조하세요.

[S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다

관련 요구 사항: 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)

범주: 보호 > 데이터 보호

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-lifecycle-policy-check

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `targetTransitionDays` | 객체 생성 후 객체를 지정된 스토리지 클래스로 전환하는 시기까지의 일수 | Integer | `1~36500` | 기본값 없음 |
| `targetExpirationDays` | 객체 생성 후 객체가 삭제되는 시기까지의 일수 | Integer | `1~36500` | 기본값 없음 |
| `targetTransitionStorageClass` | 대상 S3 스토리지 클래스 유형 | Enum | `STANDARD_IA`, `INTELLIGENT_TIERING`, `ONEZONE_IA`, `GLACIER`, `GLACIER_IR`, `DEEP_ARCHIVE` | 기본값 없음 |

이 제어는 Amazon S3 범용 버킷에 수명 주기 구성이 있는지 확인합니다. 버킷에 수명 주기 구성이 없는 경우, 제어가 실패합니다. 위 파라미터 중 하나 이상에 사용자 지정 값을 제공하는 경우, 정책에 지정된 스토리지 클래스, 삭제 시간 또는 전환 시간이 포함된 경우에만 제어가 통과합니다.

S3 버킷에 수명 주기 구성을 생성하는 것은 객체 수명 동안 Amazon S3가 수행할 작업을 정의합니다. 예를 들어, 객체를 다른 스토리지 클래스로 전환하거나, 보관하거나, 지정된 기간 후에 삭제할 수 있습니다.

문제 해결

Amazon S3 버킷의 수명 주기 정책 구성에 대한 자세한 내용은 Amazon S3 사용 설명서의 버킷에 수명 주기 구성 설정 및 스토리지 수명 주기 관리를 참조하세요.

[S3.14] S3 범용 버킷에는 버전 관리가 활성화되어 있어야 합니다

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

관련 요구 사항: 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-5(2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13(5), NIST.800-171.r2 3.3.8

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-versioning-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷에 버전 관리가 활성화되어 있는지 확인합니다. 버킷의 버전 관리가 일시 중지되면 제어가 실패합니다.

버전 관리는 동일한 S3 버킷에 객체의 여러 변형을 유지합니다. 버전 관리를 사용하여 S3 버킷에 저장된 모든 객체의 모든 버전을 보존, 검색 및 복원할 수 있습니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다.

> **Tip**
>
> 수명 주기 관리 없이 버전 관리를 활성화하면 스토리지가 무제한으로 증가하고 비용이 증가할 수 있습니다. 객체를 수정할 때마다 무기한 보관되는 새 버전이 생성됩니다. 비최신 버전을 더 저렴한 스토리지 클래스로 자동 전환하거나 정의된 보존 기간 후에 만료하도록 S3 수명 주기 규칙을 구성합니다. 자세한 내용은 S3 수명 주기와 함께 S3 버전 관리 사용 및 객체 수명 주기 관리를 참조하세요.

문제 해결

S3 버킷에서 버전 관리를 사용하려면 Amazon S3 사용 설명서의 버킷 버전 관리 활성화를 참조하세요.

[S3.15] S3 범용 버킷에는 Object Lock이 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

관련 요구 사항: NIST.800-53.r5 CP-6(2), PCI DSS v4.0.1/10.5.1

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-default-lock-enabled

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `mode` | S3 Object Lock 보존 모드 | Enum | `GOVERNANCE`, `COMPLIANCE` | 기본값 없음 |

이 제어는 Amazon S3 범용 버킷에 Object Lock이 활성화되어 있는지 확인합니다. 버킷에 Object Lock이 활성화되지 않은 경우, 제어가 실패합니다. `mode` 파라미터에 사용자 지정 값을 제공하면 S3 Object Lock가 지정된 보존 모드를 사용하는 경우에만 제어가 통과합니다.

S3 객체 잠금을 사용하면 WORM(Write Once Read Many) 모델을 사용하여 Object Lock를 저장할 수 있습니다. Object Lock은 S3 버킷의 객체가 고정된 시간 동안 또는 무기한 삭제되거나 덮어쓰이는 것을 방지하는 데 도움이 됩니다. S3 Object Lock을 사용하면 WORM 스토리지가 필요한 규제 요구 사항을 충족하거나 객체 변경 및 삭제에 대한 보호 계층을 추가할 수 있습니다.

문제 해결

새로운 및 기존 S3 버킷의 Object Lock을 구성하려면 Amazon S3 사용 설명서의 S3 Object Lock 구성을 참조하세요.

[S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

관련 요구 사항: 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, NIST.800-171.r2 3.8.9, NIST.800-171.r2 3.13.11, NIST.800-171.r2 3.13.16, PCI DSS v4.0.1/3.5.1

심각도: 중간

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-default-encryption-kms

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷이 AWS KMS key (SSE-KMS 또는 DSSE-KMS)로 암호화되었는지 확인합니다. 버킷을 기본 암호화(SSE-S3)로 암호화하면 제어가 실패합니다.

서버 측 암호화(SSE)는 데이터를 받는 애플리케이션 또는 서비스에 의해 해당 대상에서 데이터를 암호화하는 것입니다. 달리 지정하지 않는 한, S3 버킷은 서버 측 암호화에 기본적으로 Amazon S3 관리형 키(SSE-S3)를 사용합니다. 그러나 추가 제어를 위해 ( AWS KMS keys SSE-KMS 또는 DSSE-KMS)를 사용한 서버 측 암호화를 대신 사용하도록 버킷을 구성할 수 있습니다. Amazon S3는 데이터 센터의 디스크에 데이터를 쓸 때 객체 수준에서 AWS 데이터를 암호화하고 액세스할 때 데이터를 복호화합니다.

문제 해결

SSE-KMS를 사용하여 S3 버킷을 암호화하려면 Amazon S3 사용 설명서의 AWS KMS (SSE-KMS)를 사용한 서버 측 암호화 지정을 참조하세요. DSSE-KMS를 사용하여 S3 버킷을 암호화하려면 Amazon S3 사용 설명서의 AWS KMS keys (DSSE-KMS)를 사용한 이중 계층 서버 측 암호화 지정을 참조하세요.

[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::S3::AccessPoint`

AWS Config 규칙: s3-access-point-public-access-blocks

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 Access Points에 퍼블릭 액세스 차단 설정이 활성화되었는지 확인합니다. 액세스 포인트에 대해 퍼블릭 액세스 차단 설정을 활성화하지 않으면 제어가 실패합니다.

Amazon S3 Block Public Access 기능을 사용하면 계정, 버킷 및 액세스 포인트 수준의 세 가지 수준에서 S3 리소스에 대한 액세스를 관리할 수 있습니다. 각 수준의 설정을 독립적으로 구성할 수 있으므로 데이터에 대해 다양한 수준의 퍼블릭 액세스 제한을 적용할 수 있습니다. 액세스 포인트 설정은 상위 수준(액세스 포인트에 할당된 계정 수준 또는 버킷)에서 더 제한적인 설정을 개별적으로 재정의할 수 없습니다. 대신 액세스 포인트 수준의 설정은 추가적이므로 다른 수준의 설정을 보완하고 그 설정과 연동합니다. S3 액세스 포인트를 공개적으로 액세스할 수 있도록 하려는 경우가 아니라면 퍼블릭 액세스 차단 설정을 활성화해야 합니다.

문제 해결

Amazon S3에서는 현재 액세스 포인트가 생성된 후 액세스 포인트의 퍼블릭 액세스 차단 설정을 변경하도록 지원하지 않습니다. 새로운 액세스 포인트를 생성하면 기본적으로 모든 퍼블릭 액세스 차단 설정이 활성화되어 있습니다. 특정 설정을 사용 중지해야 하는 경우가 아니면 모든 설정을 그대로 유지하는 것이 좋습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 액세스 포인트에 대한 퍼블릭 액세스 관리를 참조하세요.

[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/2.1.2, CIS AWS 파운데이션 벤치마크 v3.0.0/2.1.2, CIS AWS 파운데이션 벤치마크 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)

범주: 보호 > 데이터 보호 > 데이터 삭제 보호

심각도: 낮음

리소스 유형: `AWS::S3::Bucket`

AWS Config 규칙: s3-bucket-mfa-delete-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 범용 버킷에서 다중 인증(MFA) 삭제가 활성화되었는지 여부를 확인합니다. 버킷에서 MFA Delete가 활성화되지 않은 경우 제어가 실패합니다. 제어는 수명 주기 구성이 있는 버킷에 대한 조사 결과를 생성하지 않습니다.

S3 범용 버킷에 대해 버전 관리를 활성화하는 경우, 선택적으로 버킷에 대해 MFA Delete를 구성하여 다른 보안 계층을 추가할 수 있습니다. 이렇게 하는 경우 버킷 소유자는 버킷 내 객체의 특정 버전을 삭제하거나 버킷의 버전 관리 상태를 변경하는 모든 요청에 두 가지 형식의 인증을 포함해야 합니다. MFA Delete는 예를 들어 버킷 소유자의 보안 자격 증명이 손상된 경우에 대비하여 보안을 강화합니다. 또한 MFA Delete는 삭제 작업을 시작하는 사용자에게 MFA 코드를 통해 MFA 디바이스의 물리적 소유를 증명할 것을 요구하여 삭제 작업에 추가 마찰 및 보안 계층을 추가합니다. 따라서 실수로 인한 버킷 삭제를 방지하는 데 도움이 될 수 있습니다.

> **Note**
>
> 이 제어는 S3 범용 버킷에서 MFA Delete가 활성화된 경우에만 `PASSED` 조사 결과를 생성합니다. 버킷에 대해 MFA Delete를 활성화하려면 해당 버킷에서 버전 관리도 활성화해야 합니다. 버킷 버전 관리는 동일 버킷 내에 여러 개의 S3 객체 변형을 저장하는 방법입니다. 또한 루트 사용자로 로그인한 버킷 소유자만 MFA Delete를 활성화하고 버킷에서 삭제 작업을 수행할 수 있습니다. 수명 주기 구성이 있는 버킷에는 MFA Delete를 사용할 수 없습니다.

문제 해결

S3 버킷에서 버전 관리를 활성화하고 MFA Delete를 구성하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 MFA Delete 구성을 참조하세요.

[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/3.8, CIS AWS 파운데이션 벤치마크 v3.0.0/3.8, PCI DSS v4.0.1/10.2.1

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: cloudtrail-all-write-s3-data-event-check

스케줄 유형: 주기적

파라미터: 없음

이 제어 AWS 계정 는에 Amazon S3 버킷에 대한 모든 쓰기 데이터 이벤트를 로깅하는 AWS CloudTrail 다중 리전 추적이 하나 이상 있는지 확인합니다. 계정에 S3 버킷에 대한 쓰기 데이터 이벤트를 로그하는 다중 리전 추적이 없는 경우, 제어가 실패합니다.

`GetObject`, `DeleteObject`, 및 `PutObject`과 같은 S3 객체 수준 작업을 데이터 이벤트라고 합니다. 기본적으로 CloudTrail은 데이터 이벤트를 기록하지 않지만 S3 버킷에 대한 데이터 이벤트를 기록하도록 추적을 구성할 수 있습니다. 쓰기 데이터 이벤트에 대해 객체 수준 로깅을 활성화하면 S3 버킷 내에서 각 개별 객체(파일) 액세스를 기록할 수 있습니다. 객체 수준 로깅을 활성화하면 Amazon CloudWatch Events를 사용하여 데이터 규정 준수 요구 사항을 충족하고, 포괄적인 보안 분석을 수행하고,에서 특정 사용자 동작 패턴을 모니터링하고 AWS 계정, S3 버킷 내의 객체 수준 API 활동에 대한 조치를 취하는 데 도움이 될 수 있습니다. 이 제어는 모든 S3 버킷에 대해 쓰기 전용 또는 모든 유형의 데이터 이벤트를 로깅하는 다중 리전 추적을 구성하는 경우, `PASSED` 조사 결과를 생성합니다.

문제 해결

S3 버킷에 대한 객체 수준 로깅을 활성화하려면 Amazon Simple Storage Service 사용 설명서의 S3 버킷 및 객체에 대한 CloudTrail 이벤트 로깅 활성화를 참조하세요.

[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.

관련 요구 사항: CIS AWS 파운데이션 벤치마크 v5.0.0/3.9, CIS AWS 파운데이션 벤치마크 v3.0.0/3.9, PCI DSS v4.0.1/10.2.1

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: cloudtrail-all-read-s3-data-event-check

스케줄 유형: 주기적

파라미터: 없음

이 제어 AWS 계정 는에 Amazon S3 버킷에 대한 모든 읽기 데이터 이벤트를 로깅하는 AWS CloudTrail 다중 리전 추적이 하나 이상 있는지 확인합니다. 계정에 S3 버킷에 대한 읽기 데이터 이벤트를 로그하는 다중 리전 추적이 없는 경우, 제어가 실패합니다.

GetObject, DeleteObject, 및 PutObject과 같은 S3 객체 수준 작업을 데이터 이벤트라고 합니다. 기본적으로 CloudTrail은 데이터 이벤트를 기록하지 않지만 S3 버킷에 대한 데이터 이벤트를 기록하도록 추적을 구성할 수 있습니다. 읽기 데이터 이벤트에 대해 객체 수준 로깅을 활성화하면 S3 버킷 내에서 각 개별 객체(파일) 액세스를 기록할 수 있습니다. 객체 수준 로깅을 활성화하면 Amazon CloudWatch Events를 사용하여 데이터 규정 준수 요구 사항을 충족하고, 포괄적인 보안 분석을 수행하고,에서 특정 사용자 동작 패턴을 모니터링하고 AWS 계정, S3 버킷 내의 객체 수준 API 활동에 대한 조치를 취하는 데 도움이 될 수 있습니다. 이 제어는 모든 S3 버킷에 대해 읽기 전용 또는 모든 유형의 데이터 이벤트를 기록하는 다중 리전 추적을 구성하는 경우, PASSED 조사 결과를 생성합니다.

문제 해결

S3 버킷에 대한 객체 수준 로깅을 활성화하려면 Amazon Simple Storage Service 사용 설명서의 S3 버킷 및 객체에 대한 CloudTrail 이벤트 로깅 활성화를 참조하세요.

[S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다

관련 요구 사항: PCI DSS v4.0.1/1.4.4

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: AWS::S3::MultiRegionAccessPoint

AWS Config 규칙: s3-mrap-public-access-blocked (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon S3 다중 리전 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되었는지 확인합니다. 다중 리전 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있지 않으면 제어가 실패합니다.

공개적으로 액세스 가능한 리소스는 무단 액세스, 데이터 침해 또는 취약성 악용을 초래할 수 있습니다. 인증 및 권한 부여 조치를 통해 액세스를 제한하면 민감한 정보를 보호하고 리소스의 무결성을 유지하는 데 도움이 됩니다.

문제 해결

S3 다중 리전 액세스 포인트에는 기본값으로 모든 퍼블릭 액세스 차단 설정이 사용 설정되어 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 안내서의 Amazon S3 다중 리전 액세스 포인

트를 사용한 퍼블릭 액세스 차단를 참조하세요. 다중 리전 액세스 포인트를 만든 후에는 다중 리전 액세스 포인트의 퍼블릭 액세스 차단 설정을 변경할 수 없습니다.

[S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다

범주: 보호 > 데이터 보호

심각도: 낮음

리소스 유형: `AWS::S3Express::DirectoryBucket`

AWS Config 규칙: s3express-dir-bucket-lifecycle-rules-check

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `targetExpirationDays` | 객체 생성 후 객체가 만료되어야 하는 기간(일)입니다. | Integer | 1~2147483647 | 기본값 없음 |

이 제어는 S3 디렉터리 버킷에서 수명 주기 규칙이 구성되어 있는지 확인합니다. 디렉터리 버킷에 수명 주기 규칙이 구성되지 않았거나 버킷에 대한 수명 주기 규칙이 선택적으로 지정하는 파라미터 값과 일치하지 않는 만료 설정을 지정하는 경우 제어가 실패합니다.

Amazon S3에서 수명 주기 구성은 Amazon S3가 버킷의 객체 그룹에 적용하는 작업을 정의하는 일련의 규칙입니다. S3 디렉터리 버킷의 경우 수명(일)을 기준으로 객체가 만료되는 시점을 지정하는 수명 주기 규칙을 생성할 수 있습니다. 미완료 멀티파트 업로드를 삭제하는 수명 주기 규칙도 생성할 수 있습니다. 범용 버킷과 같은 다른 유형의 S3 버킷과 달리 디렉터리 버킷은 스토리지 클래스 간 객체 전환과 같은 다른 유형의 수명 주기 규칙 작업을 지원하지 않습니다.

문제 해결

S3 디렉터리 버킷에서 수명 주기 구성을 정의하려면 버킷에 대한 수명 주기 규칙을 생성합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 디렉터리 버킷에 대한 수명 주기 구성 생성 및 관리를 참조하세요.

## SageMaker AI에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM 제어는 Amazon SageMaker AI 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다 AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 네트워크 구성

심각도: 높음

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: sagemaker-notebook-no-direct-internet-access

스케줄 유형: 주기적

파라미터: 없음

이 제어는 SageMaker AI 노트북 인스턴스에 대해 직접 인터넷 액세스가 비활성화되어 있는지 확인합니다. 노트북 인스턴스에 `DirectInternetAccess` 필드가 활성화된 경우, 제어가 실패합니다.

VPC 없이 SageMaker AI 인스턴스를 구성하는 경우, 기본적으로 인스턴스에서 직접 인터넷 액세스가 활성화됩니다. VPC로 인스턴스를 구성하고 기본 설정을 비활성화-VPC를 통해 인터넷에 액세스로 변경해야 합니다. 노트북에서 모델을 훈련하거나 호스팅하려면 인터넷 액세스가 필요합니다. 인터넷 액세스를 활성화하려면 VPC에 인터페이스 엔드포인트(AWS PrivateLink) 또는 NAT 게이트웨이와 아웃바운드 연결을 허용하는 보안 그룹이 있어야 합니다. 노트북 인스턴스를 VPC의 리소스에 연결하는 방법에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 노트북 인스턴스를 VPC의 리소스에 연결하는 방법을 참조하세요. 또한 SageMaker AI 구성에 대한 액세스가 인증된 사용자로만 제한되도록 해야 합니다. 사용자가 SageMaker AI 설정 및 리소스를 변경할 수 있도록 허용하는 IAM 권한을 제한합니다.

문제 해결

노트북 인스턴스를 생성한 후에는 인터넷 액세스 설정을 변경할 수 없습니다. 대신 인터넷 액세스가 차단된 인스턴스를 중지, 삭제하고 다시 만들 수 있습니다. 인터넷에 직접 액세스할 수 있는 노트북 인스턴스를 삭제하려면 Amazon SageMaker AI 개발자 안내서의 노트북 인스턴스를 사용하여 모델 구축: 정리를 참조하세요. 인터넷 액세스를 거부하는 노트북 인스턴스를 다시 생성하려면 노트북 인스턴스 생성을 참조하세요. 네트워크, 직접 인터넷 액세스에서 비활성화 - VPC를 통해 인터넷 액세스를 선택합니다.

[SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 높음

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: sagemaker-notebook-instance-inside-vpc

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 노트북 인스턴스가 사용자 지정 가상 프라이빗 클라우드(VPC) 내에서 시작되었는지 여부를 확인합니다. SageMaker AI 노트북 인스턴스가 사용자 지정 VPC 내에서 시작되지 않거나 SageMaker AI 서비스 VPC에서 시작된 경우, 이 제어가 실패합니다.

서브넷은 VPC 내의 IP 주소 범위입니다. 인프라의 안전한 네트워크 보호를 위해 가능하면 리소스를 사용자 지정 VPC에 보관하는 것이 좋습니다. Amazon VPC는 전용 가상 네트워크입니다 AWS 계정. Amazon VPC를 사용하면 SageMaker AI Studio 및 노트북 인스턴스의 네트워크 액세스 및 인터넷 연결을 제어할 수 있습니다.

문제 해결

노트북 인스턴스를 만든 후에는 VPC 설정을 변경할 수 없습니다. 대신 인스턴스를 중지, 삭제 및 다시 만들 수 있습니다. 지침은 Amazon SageMaker AI 개발자 안내서의 노트북 인스턴스를 사용하여 모델 구축: 정리를 참조하세요.

[SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 액세스 관리 > 루트 사용자 액세스 제한

심각도: 높음

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: sagemaker-notebook-instance-root-access-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 노트북 인스턴스에 대한 루트 액세스가 설정되어 있는지 여부를 확인합니다. SageMaker AI 노트북 인스턴스에 대한 루트 액세스가 켜져 있는 경우 제어가 실패합니다.

최소 권한 원칙을 준수하기 위해, 의도치 않게 권한을 과도하게 프로비저닝하지 않도록 인스턴스 리소스에 대한 루트 액세스를 제한하는 것이 권장되는 보안 모범 사례입니다.

문제 해결

SageMaker AI 노트북 인스턴스에 대한 루트 액세스를 제한하려면 Amazon SageMaker AI 개발자 안내서의 SageMaker AI 노트북 인스턴스에 대한 루트 액세스 제어를 참조하세요.

[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

관련 요구 사항: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SA-13

범주: 복구 > 복원력 > 고가용성

심각도: 중간

리소스 유형: `AWS::SageMaker::EndpointConfig`

AWS Config 규칙: sagemaker-endpoint-config-prod-instance-count

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon SageMaker AI 엔드포인트의 프로덕션 변형에 초기 인스턴스 수가 1보다 큰지 확인합니다. 엔드포인트의 프로덕션 변형에 초기 인스턴스가 1개만 있는 경우, 제어가 실패합니다.

인스턴스 수가 2개 이상인 프로덕션 변형은 SageMaker AI에서 관리하는 다중 AZ 인스턴스 중복을 허용합니다. 여러 가용 영역에 리소스를 배포하는 것은 아키텍처 내에서 고가용성을 제공하는 AWS 모범 사례입니다. 고가용성은 보안 인시던트에서 복구하는 데 도움이 됩니다.

> **Note**
>
> 이 제어는 인스턴스 기반 엔드포인트 구성에만 적용됩니다.

문제 해결

다른 엔드포인트 구성 옵션에 대한 자세한 내용은 Amazon SageMaker AI 서비스 개발자 안내서의 엔드포인트 구성 생성 을 참조하세요.

[SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 중간

리소스 유형: `AWS::SageMaker::Model`

AWS Config 규칙: sagemaker-model-isolation-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 호스팅 모델에 네트워크 격리가 활성화되어 있는지 확인합니다. 호스팅 모델의 `EnableNetworkIsolation` 파라미터가 `False`로 설정된 경우 제어가 실패합니다.

SageMaker AI 훈련 및 배포된 추론 컨테이너는 기본적으로 인터넷을 사용합니다. SageMaker AI가 훈련 또는 추론 컨테이너에 대한 외부 네트워크 액세스를 제공하지 않도록 하려면 네트워크 격리를 활성화할 수 있습니다. 네트워크 격리를 활성화하면 다른 AWS 서비스와의 호출을 포함하여 모델 컨테이너와의 인바운드 또는 아웃바운드 네트워크 호출을 수행할 수 없습니다. 또한 컨테이너 런타임 환경에서

는 자격 AWS 증명을 사용할 수 없습니다. 네트워크 격리를 활성화하면 인터넷에서 SageMaker AI 리소스에 대한 의도하지 않은 액세스를 방지하는 데 도움이 됩니다.

> **Note**
>
> 2025년 8월 13일에 Security Hub CSPM은이 제어의 제목과 설명을 변경했습니다. 새로운 제목 및 설명은 제어가 Amazon SageMaker AI 호스팅 모델의 `EnableNetworkIsolation` 파라미터에 대한 설정을 확인함을 보다 정확하게 반영합니다. 이전에는 이 제어의 제목이 SageMaker models should block inbound traffic였습니다.

문제 해결

SageMaker AI 모델의 네트워크 격리에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 인터넷이 연결되지 않은 모드에서 훈련 및 추론 컨테이너 실행을 참조하세요. 모델을 생성할 때 `EnableNetworkIsolation` 파라미터 값을 `True`로 설정하여 네트워크 격리를 활성화할 수 있습니다.

[SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::SageMaker::AppImageConfig`

AWS Config 규칙: sagemaker-app-image-config-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon SageMaker AI 앱 이미지 구성(AppImageConfig)에 requiredKeyTags 파라미터에 지정된 태그 키가 있는지 확인합니다. 앱 이미지 구성에 태그 키가 없거나 requiredKeyTags 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. requiredKeyTags 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 앱 이미지 구성에 태그 키가 없는 경우 제어가 실패합니다. 제어는 aws: 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon SageMaker AI 앱 이미지 구성(AppImageConfig)에 태그를 추가하려면 SageMaker AI API의 AddTags 작업을 사용하거나를 사용하는 경우 add-tags 명령을 AWS CLI실행합니다.

[SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: AWS::SageMaker::Image

AWS Config 규칙: sagemaker-image-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon SageMaker AI 이미지에 `requiredKeyTags` 파라미터에 지정된 태그 키가 있는지 확인합니다. 이미지에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 이미지에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS 리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS 리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다 AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

Amazon SageMaker AI 이미지에 태그를 추가하려면 SageMaker AI API의 AddTags 작업을 사용하거나를 사용하는 경우 add-tags 명령을 AWS CLI실행합니다.

[SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다

범주: 감지 > 취약성, 패치 및 버전 관리

심각도: 중간

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: sagemaker-notebook-instance-platform-version

스케줄 유형: 주기적

파라미터:

- `supportedPlatformIdentifierVersions`: `notebook-al2023-v1`(사용자 지정할 수 없음)

이 제어는 Amazon SageMaker AI 노트북 인스턴스에 지정된 플랫폼 식별자를 기반으로 노트북 인스턴스가 지원되는 플랫폼에서 실행되도록 구성되어 있는지 확인합니다. 노트북 인스턴스가 더 이상 지원되지 않는 플랫폼에서 실행되도록 구성된 경우 제어가 실패합니다.

Amazon SageMaker AI 노트북 인스턴스의 플랫폼이 더 이상 지원되지 않는 경우 보안 패치, 버그 수정 또는 기타 유형의 업데이트를 수신하지 못할 수 있습니다. 노트북 인스턴스는 계속 작동할 수 있지만 SageMaker AI 보안 업데이트 또는 중요한 버그 수정은 수신되지 않습니다. 지원되지 않는 플랫폼 사용과 관련된 위험을 부담하게 됩니다. 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 JupyterLab 버전 관리를 참조하세요.

문제 해결

Amazon SageMaker AI가 현재 지원하는 플랫폼 및 해당 플랫폼으로 마이그레이션하는 방법에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 Amazon Linux 2 노트북 인스턴스를 참조하세요.

[SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::DataQualityJobDefinition`

AWS Config 규칙: sagemaker-data-quality-job-encrypt-in-transit

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 데이터 품질 작업 정의에 컨테이너 간 트래픽에 대한 암호화가 활성화되어 있는지 확인합니다. 데이터 품질 및 드리프트를 모니터링하는 작업의 정의에 컨테이너 간 트래픽에 대해 암호화가 활성화되지 않은 경우 제어가 실패합니다.

컨테이너 간 트래픽 암호화를 활성화하면 데이터 품질 분석을 위한 분산 처리 중에 민감한 ML 데이터가 보호됩니다.

문제 해결

Amazon SageMaker AI의 컨테이너 간 트래픽 암호화에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 분산 훈련 작업의 ML 컴퓨팅 인스턴스 간 통신 보호를 참조하세요. 데이터 품질 작업 정의를 생성할 때 `EnableInterContainerTrafficEncryption` 파라미터 값을 로 설정하여 컨테이너 간 트래픽 암호화를 활성화할 수 있습니다`True`.

[SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::ModelExplainabilityJobDefinition`

AWS Config 규칙: sagemaker-model-explainability-job-encrypt-in-transit

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker 모델 설명 가능성 작업 정의에 컨테이너 간 트래픽 암호화가 활성화되어 있는지 확인합니다. 모델 설명 가능성 작업 정의에 컨테이너 간 트래픽 암호화가 활성화되어 있지 않으면 제어가 실패합니다.

컨테이너 간 트래픽 암호화를 활성화하면 설명 가능성 분석을 위해 분산 처리 중에 모델 데이터, 훈련 데이터 세트, 중간 처리 결과, 파라미터 및 모델 가중치와 같은 민감한 ML 데이터를 보호할 수 있습니다.

문제 해결

기존 SageMaker 모델 설명 가능성 작업 정의의 경우 컨테이너 간 트래픽 암호화를 업데이트할 수 없습니다. 컨테이너 간 트래픽 암호화가 활성화된 상태에서 새 SageMaker 모

델 설명 가능성 작업 정의를 생성하려면 API 또는 CLI 또는 CloudFormation을 사용하고를 EnableInterContainerTrafficEncryption로 설정합니다True.

[SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: AWS::SageMaker::DataQualityJobDefinition

AWS Config 규칙: sagemaker-data-quality-job-isolation

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 데이터 품질 모니터링 작업 정의에 네트워크 격리가 활성화되어 있는지 확인합니다. 데이터 품질 및 드리프트를 모니터링하는 작업의 정의에 네트워크 격리가 비활성화된 경우 제어가 실패합니다.

네트워크 격리는 공격 표면을 줄이고 외부 액세스를 방지하여 무단 외부 액세스, 우발적인 데이터 노출 및 잠재적 데이터 유출로부터 보호합니다.

문제 해결

SageMaker AI의 네트워크 격리에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 인터넷 없는 모드에서 훈련 및 추론 컨테이너 실행을 참조하세요. 데이터 품질 작업 정의를 생성할 때 EnableNetworkIsolation 파라미터 값을 로 설정하여 네트워크 격리를 활성화할 수 있습니다True.

[SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

범주: 보호 > 보안 네트워크 구성 > 리소스 정책 구성

심각도: 중간

리소스 유형: AWS::SageMaker::ModelBiasJobDefinition

AWS Config 규칙: sagemaker-model-bias-job-isolation

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 SageMaker 모델 편향 작업 정의에 네트워크 격리가 활성화되어 있는지 확인합니다. 모델 바이어스 작업 정의에 네트워크 격리가 활성화되어 있지 않으면 제어가 실패합니다.

네트워크 격리는 SageMaker 모델 편향 작업이 인터넷을 통해 외부 리소스와 통신하는 것을 방지합니다. 네트워크 격리를 활성화하면 작업의 컨테이너가 아웃바운드 연결을 할 수 없으므로 공격 표면이 줄어들고 민감한 데이터가 유출되지 않도록 보호할 수 있습니다. 이는 규제되거나 민감한 데이터를 처리하는 작업에 특히 중요합니다.

문제 해결

네트워크 격리를 활성화하려면 `EnableNetworkIsolation` 파라미터가 로 설정된 새 모델 바이어스 작업 정의를 생성해야 합니다`True`. 작업 정의 생성 후에는 네트워크 격리를 수정할 수 없습니다. 새 모델 바이어스 작업 정의를 생성하려면 Amazon SageMaker AI 개발자 안내서의 CreateModelBiasJobDefinition을 참조하세요.

[SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::ModelQualityJobDefinition`

AWS Config 규칙: ssagemaker-model-quality-job-encrypt-in-transit

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker 모델 품질 작업 정의에 컨테이너 간 트래픽에 대해 전송 중 암호화가 활성화되어 있는지 확인합니다. 모델 품질 작업 정의에 컨테이너 간 트래픽 암호화가 활성화되어 있지 않으면 제어가 실패합니다.

컨테이너 간 트래픽 암호화는 분산 모델 품질 모니터링 작업 중에 컨테이너 간에 전송되는 데이터를 보호합니다. 기본적으로 컨테이너 간 트래픽은 암호화되지 않습니다. 암호화를 활성화하면 처리 중에 데이터 기밀을 유지하고 전송 중 데이터 보호에 대한 규제 요구 사항 준수를 지원할 수 있습니다.

문제 해결

Amazon SageMaker 모델 품질 작업 정의에 대해 컨테이너 간 트래픽 암호화를 활성화하려면 적절한 전송 중 암호화 구성으로 작업 정의를 다시 생성해야 합니다. 모델 품질 작업 정의를 생성하려면 Amazon SageMaker AI 개발자 안내서의 CreateModelQualityJobDefinition을 참조하세요.

[SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::SageMaker::MonitoringSchedule`

AWS Config 규칙: sagemaker-monitoring-schedule-isolation

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker 모니터링 일정에 네트워크 격리가 활성화되어 있는지 확인합니다. 모니터링 일정에 EnableNetworkIsolation이 false로 설정되어 있거나 구성되지 않은 경우 제어가 실패합니다.

네트워크 격리는 모니터링 작업의 아웃바운드 네트워크 호출을 방지하여 컨테이너에서 인터넷 액세스를 제거하여 공격 영역을 줄입니다.

문제 해결

모니터링 일정을 생성하거나 업데이트할 때 NetworkConfig 파라미터에서 네트워크 격리를 구성하는 방법에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 CreateMonitoringSchedule 또는 UpdateMonitoringSchedule을 참조하세요.

[SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::ModelBiasJobDefinition`

AWS Config 규칙: sagemaker-model-bias-job-encrypt-in-transit

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker 모델 바이어스 작업 정의에 여러 컴퓨팅 인스턴스를 사용할 때 컨테이너 간 트래픽 암호화가 활성화되어 있는지 확인합니다. 이 false로

`EnableInterContainerTrafficEncryption` 설정되거나 인스턴스 수가 2 이상인 작업 정의에 대해 구성되지 않은 경우 제어가 실패합니다.

컨테이너 간 트래픽 암호화는 분산 모델 편향 모니터링 작업 중에 컴퓨팅 인스턴스 간에 전송되는 데이터를 보호합니다. 암호화는 인스턴스 간에 전송되는 가중치와 같은 모델 관련 정보에 대한 무단 액세스를 방지합니다.

문제 해결

SageMaker 모델 바이어스 작업 정의에 대해 컨테이너 간 트래픽 암호화를 활성화하려면 작업 정의에서 여러 컴퓨팅 인스턴스를 사용할 `True` 때 `EnableInterContainerTrafficEncryption` 파라미터를 로 설정합니다. ML 컴퓨팅 인스턴스 간 통신 보호에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 분산 훈련 작업에서 ML 컴퓨팅 인스턴스 간 통신 보호를 참조하세요.

[SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 중간

리소스 유형: `AWS::SageMaker::Model`

AWS Config 규칙: sagemaker-model-private-registry-required

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 모델이 기본 컨테이너에 대한 VPC의 프라이빗 레지스트리에서 컨테이너 이미지를 가져오는지 확인합니다. 이미지가 구성되지 않았거나 리포지토리 액세스 모드가 인 경우 제어가 실패합니다`Platform`.

SageMaker 모델 컨테이너용 VPC에서 프라이빗 Docker 레지스트리를 사용하면 VPC 내의 신뢰할 수 있고 제어된 소스에서 컨테이너 이미지를 가져올 수 있습니다. 또한 퍼블릭 인터넷을 통과하지 않고도 VPC 엔드포인트를 통해 컨테이너 이미지에 액세스할 수 있습니다.

문제 해결

SageMaker AI 실시간 추론 컨테이너에 대한 프라이빗 도커 레지스트리를 구성하려면 Amazon SageMaker AI 개발자 안내서의 실시간 추론 컨테이너에 프라이빗 도커 레지스트리 사용을 참조하세요.

[SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::FeatureGroup`

AWS Config 규칙: sagemaker-featuregroup-encryption-at-rest

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 특성 그룹의 Amazon SageMaker 오프라인 저장소가 AWS KMS 키로 저장 시 암호화되는지 확인합니다. 특성 그룹의 오프라인 저장소 S3 스토리지가 KMS 키로 암호화되지 않은 경우 제어가 실패합니다.

SageMaker 특성 그룹 오프라인 저장소의 나머지 부분에서 암호화 AWS KMS keys 에 고객 관리형을 사용하면 보안이 강화됩니다. 고객 관리형 KMS 키를 사용하면 암호화 키 수명 주기 및 키 정책을 완벽하게 제어할 수 있습니다. 또한 모든 암호화 키 사용량은 감사 가능성을 AWS CloudTrail 위해를 통해 로깅하고 모니터링할 수 있습니다.

문제 해결

AWS KMS 고객 관리형 키를 사용하여 SageMaker 특성 저장소 오프라인 저장소에 저장 시 암호화를 활성화하는 방법에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 보안 및 액세스 제어를 참조하세요.

[SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::FeatureGroup`

AWS Config 규칙: sagemaker-featuregroup-online-store-encryption

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 표준 스토리지가 있는 특성 그룹의 Amazon SageMaker 온라인 스토어가 AWS KMS 키로 저장 시 암호화되는지 확인합니다. KMS 키 암호화가 온라인 저장소에 대해 구성되지 않은 경우 제어가 실패합니다.

SageMaker 특성 그룹 온라인 저장소의 나머지 부분에서 암호화 AWS KMS keys 에 고객 관리형을 사용하면 보안이 향상됩니다. 고객 관리형 KMS 키를 사용하면 암호화 키 수명 주기 및 키 정책을 완벽하게 제어할 수 있습니다. 또한 모든 암호화 키 사용량은 감사 가능성을 AWS CloudTrail 위해를 통해 로깅하고 모니터링할 수 있습니다.

문제 해결

AWS KMS 고객 관리형 키를 사용하여 SageMaker 특성 저장소 온라인 스토어에서 저장 시 암호화를 활성화하는 방법에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 보안 및 액세스 제어를 참조하세요.

[SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.

범주: 보호 > 보안 네트워크 구성 > VPC 내 리소스

심각도: 중간

리소스 유형: `AWS::SageMaker::Model`

AWS Config 규칙: sagemaker-model-multicontainer-private-registry

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 다중 컨테이너 추론 파이프라인이 있는 Amazon SageMaker AI 모델이 VPC의 프라이빗 Docker 레지스트리에서 컨테이너 이미지를 가져오는지 확인합니다. 컨테이너 정의에 이미지 구성이 없거나 리포지토리 액세스 모드가 플랫폼으로 설정된 경우 제어가 실패합니다.

SageMaker AI 다중 컨테이너 추론 파이프라인용 VPC에서 프라이빗 Docker 레지스트리를 사용하면 VPC 내의 신뢰할 수 있고 제어된 소스에서 컨테이너 이미지를 가져올 수 있습니다. 이렇게 하면 퍼블

릭 인터넷을 통과하지 않고도 VPC 엔드포인트를 통해 컨테이너 이미지에 액세스할 수 있으므로 공급망 공격 또는 이미지 변조 위험이 줄어듭니다.

문제 해결

SageMaker AI 실시간 추론 컨테이너에 대한 프라이빗 도커 레지스트리를 구성하려면 Amazon SageMaker AI 개발자 안내서의 실시간 추론 컨테이너에 프라이빗 도커 레지스트리 사용을 참조하세요.

[SageMaker.20] SageMaker 모델 설명 가능성 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::SageMaker::ModelExplainabilityJobDefinition`

AWS Config 규칙: sagemaker-model-explainability-job-network-isolation

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 SageMaker AI 모델 설명 가능성 작업 정의에 네트워크 격리가 활성화되어 있는지 확인합니다. 작업 정의에 네트워크 격리가 활성화되어 있지 않으면 제어가 실패합니다.

네트워크 격리는 모델 설명 가능성 작업 컨테이너가 아웃바운드 네트워크를 호출하는 것을 방지하여 데이터 유출 위험을 줄이고 민감한 모델 및 훈련 데이터에 대한 defense-in-depth를 제공합니다.

문제 해결

SageMaker AI 모델 설명 가능성 작업 정의에 대해 네트워크 격리를 활성화하려면 작업 정의를 생성할 `true` 때를 `NetworkConfig.EnableNetworkIsolation`로 설정합니다. SageMaker AI의 네트워크 격리에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 인터넷 없는 모드에서 훈련 및 추론 컨테이너 실행을 참조하세요.

[SageMaker.21] SageMaker 노트북 인스턴스는 고객 관리형 AWS KMS 키로 암호화해야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::NotebookInstance`

AWS Config 규칙: sagemaker-notebook-instance-storage-vol-kms-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 SageMaker AI 노트북 인스턴스가 스토리지 볼륨 암호화를 위한 AWS KMS 키로 구성되어 있는지 확인합니다. 노트북 인스턴스에 대해 KMS 키가 구성되지 않은 경우 제어가 실패합니다.

고객 관리형 KMS 키를 사용한 저장 데이터 암호화는 기본 AWS 관리형 암호화에 대한 추가 액세스 제어를 제공합니다. SageMaker AI 노트북 인스턴스는 ML 스토리지 볼륨에 사용자 노트북, 데이터 세트, 모델 아티팩트 및 임시 처리 데이터를 저장합니다. 고객 관리형 키를 사용하면 세분화된 키 정책 제어, 키 사용에 대한 CloudTrail 감사 로깅, 고객 제어 암호화가 필요한 프레임워크 준수를 사용할 수 있습니다.

문제 해결

SageMaker AI 노트북 인스턴스에 대한 KMS 키를 구성하려면 Amazon SageMaker AI 개발자 안내서의 노트북 인스턴스, SageMaker AI 작업 및 엔드포인트를 참조하세요. Amazon SageMaker 노트북 인스턴스 생성 시에만 설정할 `KmsKeyId` 수 있습니다. 문제를 해결하려면 KMS 키가 지정된 새 노트북 인스턴스를 생성하고 기존 인스턴스에서 데이터를 마이그레이션합니다.

[SageMaker.22] SageMaker 모니터링 일정에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::MonitoringSchedule`

AWS Config 규칙: sagemaker-monitoring-schedule-traffic-encryption

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 모니터링 일정에 컨테이너 간 트래픽에 대한 암호화가 활성화되어 있는지 확인합니다. 모니터링 작업 정의에 컨테이너 간 트래픽에 대한 암호화가 활성화되어 있지 않으면 제어가 실패합니다.

컨테이너 간 트래픽 암호화는 모니터링 작업 중에 컨테이너 간에 전송되는 데이터가 전송 중에 암호화되도록 합니다. 이 암호화가 없으면 모델 모니터링 중에 처리된 민감한 데이터가 네트워크 내에서 무단 액세스에 노출될 수 있습니다. 이 설정을 활성화하면 전송 중 데이터를 보호하기 위한 규정 준수 요구 사항을 충족하는 데 도움이 됩니다.

문제 해결

기존 SageMaker AI 모니터링 일정의 경우 컨테이너 간 트래픽 암호화를 업데이트할 수 없습니다. 컨테이너 간 트래픽 암호화가 활성화된 새 SageMaker AI 모니터링 일정을 생성하려면 API 또는 CLI 또는 CloudFormation을 사용하고 `NetworkConfig`의 `true`에서를 `EnableInterContainerTrafficEncryption`로 설정합니다`MonitoringJobDefinition`.

[SageMaker.23] SageMaker 추론 실험에는 고객 관리형 AWS KMS 키로 암호화된 인스턴스 스토리지 볼륨이 있어야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::InferenceExperiment`

AWS Config 규칙: sagemaker-inf-experiment-instance-storage-kms-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 SageMaker AI 추론 실험이 인스턴스 스토리지 볼륨 암호화를 위한 키로 AWS KMS 구성되어 있는지 확인합니다. 인스턴스 스토리지 볼륨 암호화에 KMS 키를 지정하지 않으면 제어가 실패합니다.

고객 관리형 KMS 키를 사용하여 인스턴스 스토리지 볼륨을 암호화하면 섀도우 테스트 중에 ML 컴퓨팅 인스턴스에 저장된 모델 아티팩트 및 임시 추론 데이터에 대한 중앙 집중식 키 관리, 감사 로깅 및 키 교체 제어가 가능합니다.

문제 해결

SageMaker AI 추론 실험에 대한 KMS 키를 구성하려면를 호출할 때 `KmsKey` 파라미터를 지정합니다`CreateInferenceExperiment`. 는 KMS 키 ID, ARN, 별칭 또는 별칭 ARN일 `KmsKey` 수 있습니다. SageMaker AI 실행 역할에는 키에 대한 `kms:CreateGrant` 권한이 있어야 합니다. SageMaker AI

에 고객 관리형 AWS KMS 키를 지정하는 방법에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 노트북 인스턴스, SageMaker AI 작업 및 엔드포인트를 참조하세요. Amazon SageMaker

[SageMaker.24] SageMaker 추론 실험에는 고객 관리형 AWS KMS 키로 암호화된 데이터 스토리지가 있어야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SageMaker::InferenceExperiment`

AWS Config 규칙: sagemaker-inf-experiment-data-storage-kms-encrypted

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 데이터 캡처가 활성화된 SageMaker AI 추론 실험에 저장된 캡처된 데이터를 암호화하도록 구성된 KMS 키가 있는지 확인합니다. 데이터 스토리지 구성이 암호화를 위한 KMS 키를 지정하지 않으면 제어가 실패합니다.

고객 관리형 KMS 키를 사용하여 캡처된 추론 요청 및 응답 데이터를 암호화하면 Amazon S3에 저장된 민감한 추론 페이로드를 중앙 집중식 키 관리 및 감사 기능으로 보호할 수 있습니다.

문제 해결

SageMaker AI 추론 실험에서 데이터 스토리지에 대한 KMS 키를 구성하려면를 호출`DataStorageConfig`할 때 내에서 `KmsKey` 필드를 지정합니다`CreateInferenceExperiment`. 는 지정된 Amazon S3 버킷에 저장된 캡처된 추론 요청 및 응답 데이터를 `KmsKey` 암호화합니다. SageMaker AI에 고객 관리형 AWS KMS 키를 지정하는 방법에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 노트북 인스턴스, SageMaker AI 작업 및 엔드포인트를 참조하세요. Amazon SageMaker

[SageMaker.25] SageMaker 모델 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 높음

리소스 유형: `AWS::SageMaker::ModelQualityJobDefinition`

AWS Config 규칙: sagemaker-model-quality-job-definition-isolation

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SageMaker AI 모델 품질 작업 정의에 네트워크 격리가 활성화되어 있는지 확인합니다. 모델 품질 작업 정의에 네트워크 격리가 활성화되어 있지 않으면 제어가 실패합니다.

네트워크 격리는 공격 표면을 줄이고 외부 액세스를 방지하여 무단 외부 액세스, 우발적인 데이터 노출 및 잠재적 데이터 유출로부터 보호합니다.

문제 해결

모델 품질 작업 정의를 생성할 때 `EnableNetworkIsolation` 파라미터 값을 로 설정하여 네트워크 격리를 활성화할 수 있습니다`True`. SageMaker AI의 네트워크 격리에 대한 자세한 내용은 Amazon SageMaker AI 개발자 안내서의 인터넷 없는 모드에서 훈련 및 추론 컨테이너 실행을 참조하세요.

## Secrets Manager에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWS Secrets Manager서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[SecretsManager.1] Secrets Manager 암호에는 자동 교체가 활성화되어 있어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 개발

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `secretsmanager-rotation-enabled-check`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `maximumAllowedRotationFrequency` | 보안 암호 교체 빈도에 허용되는 최대 일수 | Integer | `1~365` | 기본값 없음 |

이 제어는에 저장된 보안 AWS Secrets Manager암호가 자동 교체로 구성되어 있는지 확인합니다. 암호가 자동 교체로 구성되지 않은 경우, 제어가 실패합니다. `maximumAllowedRotationFrequency` 파라미터에 사용자 지정 값을 제공하는 경우, 지정된 시간 내에 보안 암호가 자동으로 교체되는 경우에만 제어가 통과합니다.

Secrets Manager는 조직의 보안 태세를 개선하는 데 도움이 됩니다. 암호에는 데이터베이스 보안 인증, 비밀번호, 타사 API 키가 포함됩니다. Secrets Manager를 사용하여 암호를 중앙에 저장하고, 암호를 자동으로 암호화하고, 암호에 대한 액세스를 제어하고, 암호를 안전하고 자동으로 교체할 수 있습니다.

Secrets Manager는 암호를 교체할 수 있습니다. 교체를 통해 장기 암호를 단기 암호로 대체할 수 있습니다. 암호를 교체하면 권한이 없는 사용자가 손상된 암호를 사용할 수 있는 기간이 제한됩니다. 이러한 이유 때문에 보안 암호는 자주 교체해야 합니다. 교체에 대한 자세한 내용은 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager보안 암호 교체를 참조하세요.

문제 해결

Secrets Manager 보안 암호의 자동 교체를 켜려면 AWS Secrets Manager사용 설명서의 콘솔을 사용하여 AWS Secrets Manager보안 암호의 자동 교체 설정을 참조하세요. 교체를 위해 AWS Lambda함수를 선택하고 구성해야 합니다.

[SecretsManager.2] 자동 교체로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 개발

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `secretsmanager-scheduled-rotation-success-check`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Secrets Manager보안 암호가 교체 일정에 따라 성공적으로 교체되었는지 확인합니다. `RotationOccurringAsScheduled` 이 `false`이면 제어는 실패합니다. 제어는 교체가 설정되어 있는 암호만 평가합니다.

Secrets Manager는 조직의 보안 태세를 개선하는 데 도움이 됩니다. 암호에는 데이터베이스 보안 인증, 비밀번호, 타사 API 키가 포함됩니다. Secrets Manager를 사용하여 암호를 중앙에 저장하고, 암호를 자동으로 암호화하고, 암호에 대한 액세스를 제어하고, 암호를 안전하고 자동으로 교체할 수 있습니다.

Secrets Manager는 암호를 교체할 수 있습니다. 교체를 통해 장기 암호를 단기 암호로 대체할 수 있습니다. 암호를 교체하면 권한이 없는 사용자가 손상된 암호를 사용할 수 있는 기간이 제한됩니다. 이러한 이유 때문에 보안 암호는 자주 교체해야 합니다.

암호가 자동으로 교체되도록 구성하는 것 외에도 순환 일정에 따라 암호가 성공적으로 교체되도록 해야 합니다.

교체에 대해 자세히 알아보려면 AWS Secrets Manager 사용 설명서의 AWS Secrets Manager 암호 교체를 참조하세요.

문제 해결

자동 교체가 실패할 경우, Secrets Manager에서 구성 오류가 발생했을 수 있습니다. Secret Manager에서 보안 암호를 교체하려면 해당 보안 암호를 소유하고 있는 데이터베이스 또는 서비스와의 상호 작용 방식을 정의하는 Lambda 함수를 사용해야 합니다.

보안 암호 교체와 관련된 일반적인 오류를 진단하고 수정하는 데 도움이 필요하면 AWS Secrets Manager사용 설명서의 보안 암호 AWS Secrets Manager교체 문제 해결을 참조하세요.

[SecretsManager.3] 사용하지 않는 Secrets Manager 암호 삭제

관련 요구 사항: NIST.800-53.r5 AC-2(1), NIST.800-53.r5 AC-3(15)

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: `secretsmanager-secret-unused`

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `unusedForDays` | 보안 암호를 사용하지 않은 상태로 유지할 수 있는 최대 일수 | Integer | `1~365` | `90` |

이 제어는 지정된 기간 내에 AWS Secrets Manager보안 암호에 액세스했는지 확인합니다. 보안 암호를 지정된 기간 이후에 사용하지 않으면 제어가 실패합니다. 액세스 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 90일을 사용합니다.

사용하지 않는 암호를 삭제하는 것은 암호를 교체하는 것만큼이나 중요합니다. 사용하지 않는 암호는 더 이상 해당 암호에 액세스할 필요가 없는 이전 사용자에 의해 악용될 수 있습니다. 또한 더 많은 사용자가 암호에 액세스할 수 있게 되면 누군가가 이를 잘못 처리하여 승인되지 않은 엔터티에 유출했을 수 있으며, 이로 인해 남용의 위험이 커집니다. 사용하지 않는 암호를 삭제하면 더 이상 필요하지 않은 사용자의 암호 액세스를 취소하는 데 도움이 됩니다. 또한 Secrets Manager를 사용하는 비용을 줄이는 데도 도움이 됩니다. 따라서 사용하지 않는 암호는 정기적으로 삭제해야 합니다.

문제 해결

비활성 Secrets Manager 보안 암호를 삭제하려면 AWS Secrets Manager사용 설명서의 AWS Secrets Manager보안 암호 삭제를 참조하세요.

[SecretsManager.4] Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config 규칙: secretsmanager-secret-periodic-rotation

스케줄 유형: 주기적

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| maxDaysSinceRotation | 보안 암호를 변경하지 않은 상태로 유지할 수 있는 최대 일수 | Integer | 1~180 | 90 |

이 제어는 AWS Secrets Manager보안 암호가 지정된 기간 내에 한 번 이상 교체되는지 확인합니다. 보안 암호를 이 정도로 자주 교체하지 않으면 제어가 실패합니다. 교체 기간에 대한 사용자 지정 파라미터 값을 제공하지 않는 한 Security Hub CSPM은 기본값인 90일을 사용합니다.

암호 회전은 AWS 계정에서 암호가 무단으로 사용되는 위험을 줄이는 데 도움이 될 수 있습니다. 그 예로는 데이터베이스 보안 인증 정보, 비밀번호, 타사 API 키, 심지어 임의의 텍스트도 포함됩니다. 오랜 기간 동안 보안 암호를 바꾸지 않으면 보안 암호가 손상될 가능성이 높아집니다.

더 많은 사용자가 보안 암호에 액세스할 수 있으므로 누군가가 잘못 취급하여 승인되지 않은 엔터티에 유출할 가능성이 높아질 수 있습니다. 보안 암호는 로그 및 캐시 데이터를 통해 유출될 수 있습니다. 디버깅 목적으로 보안 암호를 공유할 수 있으며, 디버깅이 끝나도 보안 암호를 변경하거나 취소하지 않습니다. 이러한 모든 이유로 보안 암호는 자주 교체해야 합니다.

AWS Secrets Manager에서 암호 자동 순환을 구성할 수 있습니다. 자동 교체를 사용하면 장기 암호를 단기 암호로 대체하여 손상 위험을 크게 줄일 수 있습니다. Secrets Manager 비밀에 대한 자동 교체를 구성하는 것이 좋습니다. 자세한 내용은 AWS Secrets Manager 사용 설명서에서 AWS Secrets Manager 암호 교체를 참조하세요.

문제 해결

Secrets Manager 보안 암호의 자동 교체를 켜려면 AWS Secrets Manager사용 설명서의 콘솔을 사용하여 AWS Secrets Manager보안 암호의 자동 교체 설정을 참조하세요. 교체를 위해 AWS Lambda함수를 선택하고 구성해야 합니다.

[SecretsManager.5] Secrets Manager 보안 암호에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::SecretsManager::Secret`

AWS Config규칙: `tagged-secretsmanager-secret` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS Secrets Manager보안 암호에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 보안 암호에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 보안 암호에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Secrets Manager 보안 암호에 태그를 추가하려면 AWS Secrets Manager사용 설명서의 AWS Secrets Manager보안 암호 태그 지정을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Service Catalog

이 AWS Security Hub CSPM제어는 AWS Service Catalog서비스 및 리소스를 평가합니다. 일부 AWS 리전에서는 이 제어를 사용하지 못할 수도 있습니다. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.

관련 요구 사항: 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

범주: 보호 > 보안 액세스 관리

심각도: 중간

리소스 유형: `AWS::ServiceCatalog::Portfolio`

AWS Config 규칙: service-catalog-shared-within-organization

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 와의AWS Organizations 통합이 활성화된 경우가 조직 내에서 포트폴리오를 AWS Service Catalog공유하는지 여부를 확인합니다. 조직 내에서 포트폴리오를 공유하지 않으면 제어가 실패합니다.

Organizations 내에서만 포트폴리오를 공유하면 포트폴리오가 잘못된 AWS 계정와 공유되지 않도록 하는 데 도움이 됩니다. 조직의 계정과 Service Catalog 포트폴리오를 공유하려면 Security Hub CSPM은 `ORGANIZATION_MEMBER_ACCOUNT` 대신를 사용할 것을 권장합니다`ACCOUNT`. 이렇게 하면 조직 전체에서 계정에 부여된 액세스를 관리하여 관리를 간소화할 수 있습니다. 외부 계정과 서비스 카탈로그 포트폴리오를 공유해야 하는 비즈니스 요구가 있는 경우, 이 제어에서 조사 결과를 자동으로 억제 또는 비활성화할 수 있습니다.

문제 해결

와의 포트폴리오 공유를 활성화하려면 AWS Service Catalog관리자 안내서의 와 공유AWS Organizations를 AWS Organizations참조하세요.

## Amazon SES에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Simple Email Service(Amazon SES) 서비스 및 리소스를 평가합니다.

이러한 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[SES.1] SES 연락처 목록에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::SES::ContactList`

AWS Config규칙: `tagged-ses-contactlist` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon SES 연락처 목록에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 연락처 목록에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 연락처에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는

데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Amazon SES 연락처 목록에 태그를 추가하려면 Amazon SES API v2 참조의 TagResource를 참조하세요.

[SES.2] SES 구성 세트에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::SES::ConfigurationSet`

AWS Config규칙: `tagged-ses-configurationset` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 Amazon SES 구성 세트에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 구성 세트에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 구성 세트에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Amazon SES 구성 세트에 태그를 추가하려면 Amazon SES API v2 참조의 TagResource를 참조하세요.

[SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SES::ConfigurationSet`

AWS Config 규칙: ses-sending-tls-required

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SES 구성 세트에 TLS 연결이 필요한지 여부를 확인합니다. 구성 세트에 `'REQUIRE'` 대해 TLS 정책이 로 설정되지 않으면 제어가 실패합니다.

기본적으로 Amazon SES는 기회론적 TLS를 사용합니다. 즉, 수신 메일 서버와 TLS 연결을 설정할 수 없는 경우 이메일을 암호화하지 않고 전송할 수 있습니다. 이메일 전송을 위해 TLS를 적용하면 암호화된 보안 연결을 설정할 수 있는 경우에만 메시지가 전송됩니다. 이렇게 하면 Amazon SES와 수신자의 메일 서버 간에 전송하는 동안 이메일 콘텐츠의 기밀성과 무결성을 보호할 수 있습니다. 보안 TLS 연결을 설정할 수 없는 경우 메시지가 전송되지 않아 민감한 정보의 잠재적 노출을 방지합니다.

> **Note**
>
> TLS 1.3은 Amazon SES의 기본 전송 방법이지만 구성 세트를 통해 TLS 요구 사항을 적용하지 않으면 TLS 연결이 실패할 경우 메시지가 일반 텍스트로 전달될 수 있습니다. 이 제어를 전달하려면 SES 구성 세트의 전송 옵션`'REQUIRE'`에서 TLS 정책을 로 구성해야 합니다. TLS가 필요한 경우 수신 메일 서버와 TLS 연결을 설정할 수 있는 경우에만 메시지가 전송됩니다.

문제 해결

구성 세트에 TLS 연결이 필요하도록 Amazon SES를 구성하려면 Amazon SES 개발자 안내서의 Amazon SES 및 보안 프로토콜을 참조하세요. Amazon SES

## Amazon SNS에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Simple Notification Service(Amazon SNS) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[SNS.1] SNS 주제는를 사용하여 유휴 시 암호화되어야 합니다.AWS KMS

관련 요구 사항: 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, NIST.800-171.r2 3.13.16

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SNS::Topic`

AWS Config 규칙: `sns-encrypted-kms`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Key Management Service (AWS KMS)에서 관리되는 키를 사용하여 저장 상태에서 Amazon SNS 주제가 암호화되었는지 여부를 확인합니다. SNS 주제가 서버 측 암호화(SSE)에 KMS 키를 사용하지 않는 경우, 제어가 실패합니다. 기본적으로 SNS는 디스크 암호화를 사용하여 메시지와 파일을 저장합니다. 이 제어를 전달하려면 대신 암호화에 KMS 키를 사용하도록 선택해야 합니다. 이렇게 하면 보안 계층이 추가되고 액세스 제어 유연성이 향상됩니다.

저장 데이터를 암호화하면 인증되지 않은 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다AWS. 예를 들어 데이터를 읽기 전에 해독하려면 API 권한이 필요합니다. 보안 계층을 강화하려면 KMS 키를 사용하여 SNS 주제를 암호화하는 것이 좋습니다.

문제 해결

SNS 주제에 대해 SSE를 활성화하려면 Amazon Simple Nocation Service 개발자 안내서의 Amazon SNS 주제에 대해 서버 측 암호화(SSE) 활성화를 참조하세요. SSE를 사용하려면 먼저 주제 암호화와 메시지 암호화 및 복호화를 허용하는 AWS KMS key정책도 구성해야 합니다. 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 AWS KMS권한 구성을 참조하세요.

[SNS.2] 주제에 전송된 알림 메시지에 대해 전송 상태 로깅이 활성화되어야 합니다

> **Important**
>
> Security Hub CSPM은 2024년 4월에이 제어를 사용 중지했습니다. 자세한 내용은 Security Hub CSPM 제어의 변경 로그 단원을 참조하십시오.

관련 요구 사항: NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::SNS::Topic`

AWS Config 규칙: `sns-topic-message-delivery-notification-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 엔드포인트에 대해 Amazon SNS 주제로 전송된 알림 메시지의 전송 상태에 대한 로깅이 활성화되어 있는지 확인합니다. 메시지에 대한 전송 상태 알림이 활성화되지 않은 경우, 이 제어가 실패합니다.

로깅은 서비스의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 메시지 전달 상태를 로깅하면 다음과 같은 운영 상의 인사이트를 제공하는 데 도움이 됩니다.

- 메시지가 Amazon SNS 엔드포인트에 전송되었는지 확인
- Amazon SNS 엔드포인트에서 Amazon SNS로 전송된 응답 식별
- 메시지 체류 시간(게시 타임스탬프와 Amazon SNS 엔드포인트로 전달되는 시간 사이의 시간)을 결정합니다.

문제 해결

주제에 대한 전송 상태 로깅을 구성하려면 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 메시지 전송 상태를 참조하세요.

[SNS.3] SNS 주제에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::SNS::Topic`

AWS Config규칙: `tagged-sns-topic` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | `No default value` |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon SNS 주제에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 주제에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 주제에 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

SNS 주제에 태그를 추가하려면 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS 주제 태그 구성을 참조하세요.

[SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::SNS::Topic`

AWS Config 규칙: sns-topic-no-public-access

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SNS 주제 액세스 정책이 퍼블릭 액세스를 허용하는지 확인합니다. SNS 주제 액세스 정책에서 퍼블릭 액세스를 허용하는 경우, 이 제어가 실패합니다.

Amazon SNS 액세스 정책을 특정 주제와 함께 사용하여 해당 주제를 작업할 수 있는 사람(예: 해당 주제에 메시지를 게시할 수 있는 사람 또는 해당 주제를 구독할 수 있는 사람)을 제한합니다. SNS 정책은 다른 AWS 계정또는 자체 내의 사용자에게 액세스 권한을 부여할 수 있습니다AWS 계정. 주제 정책 `Principal` 필드에 와일드카드(*)를 제공하고 주제 정책을 제한할 조건이 부족하면 데이터 유출, 서비스 거부 또는 공격자가 서비스에 메시지를 원치 않게 삽입할 수 있습니다.

> **Note**
>
> 이 제어는 와일드카드 문자 또는 변수를 사용하는 정책 조건을 평가하지 않습니다. `PASSED` 조사 결과를 생성하려면 주제에 대한 Amazon SNS 액세스 정책의 조건이 고정 값, 즉 와일드카드 문자 또는 정책 변수를 포함하지 않는 값만 사용해야 합니다. 정책 변수에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 변수 및 태그를 참조하세요.

문제 해결

SNS 주제에 대한 액세스 정책을 업데이트하려면 Amazon Simple Notification Service 개발자 안내서의 Amazon SNS에서 액세스 관리 개요를 참조하세요.

## Amazon SQS에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon Simple Queue Service(Amazon SQS) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::SQS::Queue`

AWS Config규칙: `sqs-queue-encrypted` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SQS 대기열이 저장 시 암호화되었는지 여부를 확인합니다. 대기열이 SQS 관리형 키(SSE-SQS) 또는 AWS Key Management Service() 키(SSE-KMSAWS KMS)로 암호화되지 않으면 제어가 실패합니다.

저장 데이터를 암호화하면 권한이 없는 사용자가 디스크에 저장된 데이터에 액세스할 위험이 줄어듭니다. 서버 측 암호화(SSE)는 SQS 관리형 암호화 키(SSE-SQS) 또는 AWS KMS키(SSE-KMS)를 사용하여 SQS 대기열의 메시지 내용을 보호합니다.

문제 해결

SQS 대기열에 대한 SSE를 구성하려면 Amazon Simple Queue Service 개발자 안내서의 대기열에 대한 서버 측 암호화(SSE) 구성(콘솔)을 참조하세요.

[SQS.2] SQS 대기열에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::SQS::Queue`

AWS Config규칙: `tagged-sqs-queue` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입 | StringList(최대 6개 항목) | AWS 요구 사항을 충족하 | `No default value` |

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
| --- | --- | --- | --- | --- |
| | 니다. 태그 키는 대소문자를 구별합니다. | | 는 1~6개의 태그 키. | |

이 제어는 Amazon SQS 대기열에 파라미터 `requiredTagKeys`에 정의된 특정 키가 있는 태그가 있는지 확인합니다. 대기열에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 대기열에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Amazon SQS 콘솔을 사용하여 기존 대기열에 태그를 추가하려면 Amazon Simple Queue Service 개발자 안내서의 Amazon SQS 대기열에 대한 비용 할당 태그 구성(콘솔)을 참조하세요.

[SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::SQS::Queue`

AWS Config 규칙: sqs-queue-no-public-access

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon SQS 액세스 정책이 SQS 대기열에 대한 퍼블릭 액세스를 허용하는지 확인합니다. SQS 액세스 정책에서 대기열에 대한 퍼블릭 액세스를 허용하는 경우 이 제어가 실패합니다.

Amazon SQS 액세스 정책은 SQS 대기열에 대한 퍼블릭 액세스를 허용하여 익명 사용자 또는 인증된 AWSIAM 자격 증명이 대기열에 액세스하도록 허용할 수 있습니다. SQS 액세스 정책은 일반적으로 정책의 `Principal` 요소에 와일드카드 문자(*)를 지정하거나 대기열에 대한 액세스를 제한하는 적절한 조건을 사용하지 않거나 둘 다 사용하여 이러한 액세스를 제공합니다. SQS 액세스 정책이 퍼블릭 액세스를 허용하는 경우 서드 파티가 대기열에서 메시지 수신, 대기열로 메시지 전송, 대기열 액세스 정책 수정과 같은 태스크를 수행할 수 있습니다. 이로 인해 위협 행위자에 의한 데이터 유출, 서비스 거부, 대기열에 메시지 삽입과 같은 이벤트가 발생할 수 있습니다.

> **Note**
>
> 이 제어는 와일드카드 문자 또는 변수를 사용하는 정책 조건을 평가하지 않습니다. `PASSED` 조사 결과를 생성하려면 대기열에 대한 Amazon SQS 액세스 정책의 조건이 고정 값, 즉 와일드카드 문자 또는 정책 변수를 포함하지 않는 값만 사용해야 합니다. 정책 변수에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 변수 및 태그를 참조하세요.

문제 해결

SQS 대기열에 대한 SQS 액세스 정책을 구성하는 방법에 대한 자세한 내용은 Amazon Simple Queue Service 개발자 안내서의 Amazon SQS 액세스 정책 언어로 사용자 지정 정책 사용을 참조하세요.

## Step Functions에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWS Step Functions서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.

관련 요구 사항: PCI DSS v4.0.1/10.4.2

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::StepFunctions::StateMachine`

AWS Config 규칙: `step-functions-state-machine-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `logLevel` | 최소 로깅 수준 | Enum | `ALL`, `ERROR`, `FATAL` | 기본값 없음 |

이 제어는 AWS Step Functions상태 시스템에 로깅이 켜져 있는지 확인합니다. 상태 머신에 로깅이 켜져 있지 않으면 제어가 실패합니다. `logLevel` 파라미터에 사용자 지정 값을 제공하는 경우, 상태 머신에 지정된 로깅 수준이 켜져 있는 경우에만 제어가 통과합니다.

모니터링을 통해 Step Functions의 안정성, 가용성 및 성능을 유지할 수 있습니다. 다중 지점 실패AWS 서비스를 더 쉽게 디버깅할 수 있도록 사용하는에서 모니터링 데이터를 최대한 많이 수집해야 합니다. Step Functions 상태 머신에 대해 로깅 구성을 정의하면 Amazon CloudWatch Logs에서 실행 기록과 결과를 추적할 수 있습니다. 선택적으로 오류나 치명적인 이벤트만 추적할 수 있습니다.

문제 해결

Step Functions 상태 머신에 대한 로깅을 켜려면 AWS Step Functions 개발자 안내서의 로깅 구성을 참조하세요.

[StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태그 지정

심각도: 낮음

리소스 유형: `AWS::StepFunctions::Activity`

AWS Config규칙:`tagged-stepfunctions-activity` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Step Functions활동에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 활동에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 활동에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Step Functions 활동에 태그를 추가하려면 AWS Step Functions 개발자 안내서의 Step Functions에서 태그 지정을 참조하세요.

## Systems Manager에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 AWS Systems Manager(SSM) 서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[SSM.1] Amazon EC2 인스턴스는에서 관리해야 합니다.AWS Systems Manager

관련 요구 사항: 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)

범주: 식별 > 인벤토리

심각도: 중간

평가된 리소스: `AWS::EC2::Instance`

필요한 AWS Config기록 리소스: `AWS::EC2::Instance`, `AWS::SSM::ManagedInstanceInventory`

AWS Config 규칙: ec2-instance-managed-by-systems-manager

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 계정에서 중지되고 실행 중인 EC2 인스턴스가에서 관리되는지 확인합니다AWS Systems Manager. Systems Manager는 AWS인프라를 보고 제어하는 데 사용할 수 AWS 서비스있는 입니다.

Systems Manager는 보안과 규정 준수를 유지하는 데 도움이 되도록 중지 및 실행 중인 관리형 인스턴스를 검사합니다. 관리형 인스턴스는 Systems Manager에 사용하도록 구성된 시스템입니다. 그런 다음 Systems Manager는 탐지된 모든 정책 위반에 대해 보고하거나 수정 조치를 취합니다. 또한 Systems Manager는 관리형 인스턴스를 구성하고 유지 관리하는 데 도움이 됩니다. 자세한 내용은 AWS Systems Manager 사용 설명서를 참조하세요.

> **Note**
>
> 이 제어는에서 관리하는 AWS Elastic Disaster Recovery복제 서버 인스턴스인 EC2 인스턴스에 대한 `FAILED` 결과를 생성합니다AWS. 복제 서버 인스턴스는 소스 서버에서의 지속적인 데이터 복제를 지원하기 AWS Elastic Disaster Recovery위해에서 자동으로 시작하는 EC2 인스

턴스입니다.는 AWS의도적으로 이러한 인스턴스에서 Systems Manager(SSM) 에이전트를 제거하여 격리를 유지하고 의도하지 않은 잠재적 액세스 경로를 방지합니다.

문제 해결

를 사용한 EC2 인스턴스 관리에 대한 자세한 내용은 AWS Systems Manager사용 설명서의 Amazon EC2 호스트 관리를 AWS Systems Manager참조하세요. AWS Systems Manager콘솔의 구성 옵션 섹션에서 기본 설정을 유지하거나 원하는 구성에 필요한 대로 변경할 수 있습니다.

[SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.

관련 요구 사항: 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), NIST.800-53.r5 SI-2(4), 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

범주: 감지 > 감지 서비스

심각도: 높음

리소스 유형: `AWS::SSM::PatchCompliance`

AWS Config 규칙: ec2-managedinstance-patch-compliance-status-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 인스턴스에 패치를 설치한 후 Systems Manager 패치 준수 상태가 `COMPLIANT` 또는 `NON_COMPLIANT`인지 확인합니다. 규정 준수 상태가 `NON_COMPLIANT`인 경우, 제어가 실패합니다. 제어는 Systems Manager 패치 관리자가 관리하는 인스턴스만 확인합니다.

조직의 필요에 따라 EC2 인스턴스를 완전히 패치하면 AWS 계정의 공격 표면이 줄어듭니다.

문제 해결

Systems Manager는 패치 정책을 사용하여 관리형 인스턴스에 대한 패치를 구성할 것을 권장합니다. 또한 다음 절차에서 설명한 대로 Systems Manager 문서를 사용하여 인스턴스를 패치할 수 있습니다.

규정 미준수 패치를 해결하려면

1. https://console.aws.amazon.com/systems-manager/ AWS Systems Manager콘솔을 엽니다.

2. 노드 관리에서 명령 실행을 선택한 다음 명령 실행을 선택합니다.
3. AWS-RunPatchBaseline 옵션을 선택합니다.
4. 작업을 설치로 변경합니다.
5. 수동으로 인스턴스 선택을 선택한 다음 규정 비준수 인스턴스를 선택합니다.
6. 실행을 선택합니다.
7. 명령이 완료된 후 패치가 적용된 인스턴스의 새로운 규정 준수 상태를 모니터링하려면 탐색 창에서 규정 준수를 선택합니다.

[SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.

관련 요구 사항: 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

범주: 감지 > 감지 서비스

심각도: 낮음

리소스 유형: `AWS::SSM::AssociationCompliance`

AWS Config 규칙: ec2-managedinstance-association-compliance-status-check

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Systems Manager연결 규정 준수 상태가 인스턴스에서 연결이 실행된 `COMPLIANT` `NON_COMPLIANT` 후인지 여부를 확인합니다. 연결 규정 준수 상태가 `NON_COMPLIANT`이면 제어가 실패합니다.

State Manager 연결은 관리형 인스턴스에 할당되는 구성입니다. 이러한 구성은 인스턴스에서 관리하려는 상태를 정의합니다. 예를 들어, 연결은 인스턴스에서 안티바이러스 소프트웨어가 설치되어 실행 중이어야 하는지 또는 특정 포트가 닫혀 있어야 하는지를 지정할 수 있습니다.

State Manager 연결을 하나 이상 생성하고 나면 규정 준수 상태 정보를 즉시 볼 수 있습니다. 콘솔에서 또는 AWS CLI명령이나 해당 Systems Manager API 작업에 대한 응답으로 규정 준수 상태를 볼 수 있습니다. 연결의 경우, 구성 규정 준수에는 규정 준수 상태(`Compliant` 또는 `Non-compliant`)가 표시됩니다. 또한 연결에 할당된 심각도 수준(예: `Critical` 또는 `Medium`)도 표시됩니다.

State Manager 연결 규정 준수에 대한 자세한 내용은 AWS Systems Manager 사용자 가이드에서 State Manager 연결 규정 준수 정보를 참조하세요.

문제 해결

실패한 연결은 대상 및 시스템 관리자 문서 이름을 비롯한 다양한 요인과 관련될 수 있습니다. 이 문제를 해결하려면 먼저 연결 기록을 확인하여 연결을 식별하고 조사해야 합니다. 연결 기록을 보는 방법에 대한 지침은 AWS Systems Manager 사용 설명서의 연결 기록 보기를 참조하세요.

조사를 마친 후 연결을 편집하여 식별된 문제를 수정할 수 있습니다. 연결을 편집하여 새로운 이름, 일정, 심각도 수준 또는 대상을 지정할 수 있습니다. 연결을 편집하면가 새 버전을 AWS Systems Manager생성합니다. 연결을 편집하는 방법에 대한 지침은 AWS Systems Manager 사용 설명서의 연결 편집 및 새로운 버전 생성을 참조하세요.

[SSM.4] SSM 문서는 공개해서는 안 됩니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::SSM::Document`

AWS Config 규칙: ssm-document-not-public

스케줄 유형: 주기적

파라미터: 없음

이 제어는 계정이 소유한 AWS Systems Manager문서가 퍼블릭인지 확인합니다. 소유자가 `Self`인 Systems Manager 문서가 퍼블릭이면 이 제어가 실패합니다.

공개된 시스템 관리자 문서는 문서에 의도하지 않은 액세스를 허용할 수 있습니다. 공개 시스템 관리자 문서는 계정, 리소스, 내부 프로세스에 대한 중요한 정보를 노출할 수 있습니다.

사용 사례에서 퍼블릭 공유가 필요한 경우가 아니면 소유자가 `Self`인 Systems Manager 문서에 대한 퍼블릭 공유 설정을 차단하는 것이 좋습니다.

문제 해결

Systems Manager 문서의 공유를 구성하는 방법에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 SSM 문서 공유를 참조하세요.

[SSM.5] SSM 문서에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::SSM::Document`

AWS Config 규칙: ssm-document-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Systems Manager문서에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 문서에 태그 키가 없거나 파라미터 `requiredKeyTags`에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 문서에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다. 제어는 Amazon이 소유한 Systems Manager 문서를 평가하지 않습니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC

권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS Systems Manager문서에 태그를 추가하려면 AWS Systems ManagerAPI의 AddTagsToResource 작업을 사용하거나를 사용하는 경우 add-tags-to-resource 명령을 AWS CLI실행합니다. AWS Systems Manager 콘솔을 사용할 수도 있습니다.

[SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::::Account`

AWS Config 규칙: ssm-automation-logging-enabled

스케줄 유형: 주기적

파라미터: 없음

이 제어는 Amazon CloudWatch 로깅이 AWS Systems Manager(SSM) 자동화에 대해 활성화되어 있는지 확인합니다. SSM Automation에 대해 CloudWatch 로깅이 활성화되지 않은 경우 제어가 실패합니다.

SSM Automation은 사전 정의 또는 사용자 지정 실행서를 사용하여 대규모로 AWS리소스를 배포, 구성 및 관리할 수 있는 자동화된 솔루션을 구축하는 데 도움이 되는 AWS Systems Manager도구입니다. 조직의 운영 또는 보안 요구 사항을 충족하기 위해 실행한 스크립트의 기록을 제공해야 할 수 있습니다. 런북에 있는 `aws:executeScript` 작업의 출력을 지정하는 Amazon CloudWatch Logs 로그 그룹으로 전송하도록 SSM Automation을 구성할 수 있습니다. CloudWatch Logs를 사용하면 다양한 AWS 서비스의 로그 파일을 모니터링, 저장 및 액세스할 수 있습니다.

문제 해결

SSM Automation에 대해 CloudWatch 로깅을 활성화하는 방법에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 CloudWatch Logs를 사용하여 Automation 작업 출력 로깅을 참조하세요.

[SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다

범주: 보호 > 보안 액세스 관리 > 공개적으로 액세스할 수 없는 리소스

심각도: 심각

리소스 유형: `AWS::::Account`

AWS Config 규칙: ssm-automation-block-public-sharing

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS Systems Manager 문서에 대해 퍼블릭 공유 차단 설정이 활성화되어 있는지 확인합니다. Systems Manager 문서에 대해 퍼블릭 공유 차단 설정이 비활성화된 경우 제어가 실패합니다.

AWS Systems Manager(SSM) 문서에 대한 퍼블릭 공유 차단 설정은 계정 수준 설정입니다. 이 설정을 활성화하면 SSM 문서에 대한 원치 않는 액세스를 방지할 수 있습니다. 이 설정을 활성화해도 변경 사항은 현재 일반 대중과 공유하고 있는 SSM 문서에 영향을 주지 않습니다. 사용 사례에서 일반 대중과의 문서 공유가 필요한 경우가 아니라면 SSM 문서의 퍼블릭 공유 차단 설정을 활성화하는 것이 좋습니다. 설정은 각각 다를 수 있습니다AWS 리전.

문제 해결

AWS Systems Manager(SSM) 문서에 대해 퍼블릭 공유 차단 설정을 활성화하는 방법에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 SSM 문서의 퍼블릭 공유 차단을 참조하세요.

## 에 대한 Security Hub CSPM 제어AWS Transfer Family

이러한 AWS Security Hub CSPM제어는 AWS Transfer Family서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[Transfer.1]AWS Transfer Family워크플로에 태그를 지정해야 합니다.

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Transfer::Workflow`

AWS Config규칙: `tagged-transfer-workflow` (사용자 지정 Security Hub CSPM 규칙)

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredTagKeys` | 평가된 리소스에 포함되어야 하는 비시스템 태그 키 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | `No default value` |

이 제어는 AWS Transfer Family워크플로에 파라미터에 정의된 특정 키가 있는 태그가 있는지 확인합니다`requiredTagKeys`. 워크플로에 태그 키가 없거나 파라미터 `requiredTagKeys`에 지정된 모든 키가 없는 경우, 제어가 실패합니다. 파라미터 `requiredTagKeys`이 제공되지 않은 경우, 제어는 태그 키의 존재만 확인하고 워크플로에 키로 태그가 지정되지 않은 경우 제어가 실패합니다. 자동으로 적용되고 `aws:`로 시작하는 시스템 태그는 무시됩니다.

태그는 AWS리소스에 할당하는 레이블이며 키와 선택적 값으로 구성됩니다. 태그를 생성하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그를 사용하면 리소스를 식별, 정리, 검색 및 필터링하는 데 도움을 줍니다. 태깅은 또한 작업 및 알림에 대한 책임 리소스 소유자를 추적하는 데도 도움이 됩니다. 태깅을 사용하는 경우, 속성 기반 액세스 제어(ABAC)를 태그를 기반으로 권한을 정의하는 권한 부여 전략으로 구현할 수 있습니다. IAM 엔터티(사용자 또는 역할) 및 AWS리소스에 태그를 연결할 수 있습니다. IAM 보안 주체에 대해 단일 ABAC 정책 또는 별도의 정책 세트를 생성할 수 있습니다. 이러한 ABAC 정책은 보안 주체의 태그가 리소스 태그와 일치할 때 작업을 허용하도록 설계할 수 있습니다. 자세한 내용은 ABAC란 무엇입니까AWS?를 참조하세요. IAM 사용 설명서의 .

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 추가하지 않습니다. 태그를 AWS 서비스비롯한 많은 사용자가 태그에 액세스할 수 있습니다AWS Billing. 태그 지정 모범 사례는의 AWS리소스 태그 지정을 참조하세요AWS 일반 참조.

문제 해결

Transfer Family 워크플로에 태그를 추가하려면(콘솔)

1. AWS Transfer Family콘솔을 엽니다.
2. 탐색 창에서 [워크플로(Workflows)]를 선택합니다. 그런 다음 태그를 지정할 워크플로를 선택합니다.
3. 태그 관리를 선택한 다음 태그를 추가합니다.

[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.

관련 요구 사항: 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

범주: 보호 > 데이터 보호 > 전송 중인 데이터 암호화

심각도: 중간

리소스 유형: `AWS::Transfer::Server`

AWS Config 규칙: transfer-family-server-no-ftp

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS Transfer Family서버가 엔드포인트 연결에 FTP 이외의 프로토콜을 사용하는지 확인합니다. 서버가 클라이언트가 서버의 엔드포인트에 연결하기 위해 FTP 프로토콜을 사용하는 경우, 제어가 실패합니다.

FTP(File Transfer Protocol)는 암호화되지 않은 채널을 통해 엔드포인트 연결을 설정하므로 이러한 채널을 통해 전송된 데이터는 가로채기에 취약합니다. SFTP(SSH File Transfer Protocol), FTPS(File Transfer Protocol Secure) 또는 AS2(적용성 선언문 2)를 사용하면 전송 중인 데이터를 암호화하여 추가 보안 계층을 제공할 수 있으며, 이를 사용하여 잠재적 공격자가 중간에 있는 사람 또는 유사한 공격을 사용하여 네트워크 트래픽을 도청하거나 조작하는 것을 방지할 수 있습니다.

문제 해결

Transfer Family 서버의 프로토콜을 수정하려면 AWS Transfer Family 사용 설명서의 File Transfer 프로토콜 편집을 참조하세요.

[Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다

관련 요구 사항: 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)

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::Transfer::Connector`

AWS Config 규칙: transfer-connector-logging-enabled

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS Transfer Family커넥터에 대해 Amazon CloudWatch 로깅이 활성화되어 있는지 확인합니다. 커넥터에 대해 CloudWatch 로깅이 활성화되지 않은 경우 제어가 실패합니다.

Amazon CloudWatch는 AWS Transfer Family리소스를 포함한 AWS리소스에 대한 가시성을 제공하는 모니터링 및 관찰성 서비스입니다. Transfer Family의 경우, CloudWatch는 워크플로 진행 상황 및 결과에 대한 통합 감사 및 로깅을 제공합니다. 여기에는 Transfer Family가 워크플로에 대해 정의하는 여러 지표가 포함됩니다. CloudWatch에서 자동으로 커넥터 이벤트를 로깅하도록 Transfer Family를 구성할 수 있습니다. 이렇게 하려면 커넥터에 대한 로깅 역할을 지정합니다. 로깅 역할의 경우 IAM 역할을 생성하고 해당 역할에 대한 권한을 정의하는 리소스 기반 IAM 정책을 생성합니다.

문제 해결

Transfer Family 커넥터에 대해 CloudWatch 로깅을 활성화하는 방법에 대한 자세한 내용은 AWS Transfer Family 사용 설명서의 AWS Transfer Family 서버에 대한 Amazon CloudWatch 로깅을 참조하세요.

[Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Transfer::Agreement`

AWS Config 규칙: transfer-agreement-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Transfer Family계약에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 계약에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 계약에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS Transfer Family계약에 태그를 추가하는 방법에 대한 자세한 내용은 리소스 태그 지정 및 태그 편집기 사용 설명서의 리소스 태그 지정 방법을 참조하세요. AWS

[Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Transfer::Certificate`

AWS Config 규칙: transfer-certificate-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Transfer Family인증서에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 인증서에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 인증서에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS Transfer Family인증서에 태그를 추가하는 방법에 대한 자세한 내용은 리소스 태그 지정 및 태그 편집기 사용 설명서의 리소스 태그 지정 방법을 참조하세요. AWS

[Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Transfer::Connector`

AWS Config 규칙: transfer-connector-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Transfer Family커넥터에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 커넥터에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 커넥터에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS Transfer Family커넥터에 태그를 추가하는 방법에 대한 자세한 내용은 리소스 태그 지정 및 태그 편집기 사용 설명서의 리소스 태그 지정 방법을 참조하세요. AWS

[Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다

범주: 식별 > 인벤토리 > 태깅

심각도: 낮음

리소스 유형: `AWS::Transfer::Profile`

AWS Config 규칙: transfer-profile-tagged

스케줄 유형: 변경이 트리거됨

파라미터:

| 파라미터 | 설명 | 형식 | 허용된 사용자 지정 값 | Security Hub CSPM 기본값 |
|---|---|---|---|---|
| `requiredKeyTags` | 평가된 리소스에 할당해야 하는 비시스템 태그 키의 목록입니다. 태그 키는 대소문자를 구별합니다. | StringList(최대 6개 항목) | AWS 요구 사항을 충족하는 1~6개의 태그 키. | 기본값 없음 |

이 제어는 AWS Transfer Family프로파일에 `requiredKeyTags` 파라미터로 지정된 태그 키가 있는지 확인합니다. 프로파일에 태그 키가 없거나 `requiredKeyTags` 파라미터에 지정된 모든 키가 없는 경우 제어가 실패합니다. `requiredKeyTags` 파라미터에 값을 지정하지 않는 경우, 제어는 태그 키의 존재만 확인하고 프로파일에 태그 키가 없는 경우 제어가 실패합니다. 제어는 `aws:` 접두사가 있고 자동으로 적용되는 시스템 태그를 무시합니다. 제어는 로컬 프로파일과 파트너 프로파일을 평가합니다.

태그는 사용자가 생성하고 AWS리소스에 할당하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그를 사용하여 용도, 소유자, 환경 또는 기타 기준으로 리소스를 분류할 수 있습니다. 태그는 리소스를 식별, 정리, 검색, 필터링하는 데 도움이 됩니다. 또한 작업 및 알림에 대한 리소스 소유자를 추적하는 데도 도움이 됩니다. 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 권한 부여 전략으로 구현할 수도 있습니다. ABAC 전략에 대한 자세한 내용은 IAM 사용자 설명서의 ABAC 권한 부여를 통한 속성 기반 권한 정의를 참조하세요. 태그에 대한 자세한 내용은 AWS리소스 태그 지정 및 태그 편집기 사용 설명서를 참조하세요.

> **Note**
>
> 개인 식별 정보(PII)나 기타 기밀 정보 또는 민감한 정보를 태그에 저장하지 마세요. 태그는 많은에서 액세스할 수 있습니다AWS 서비스. 태그는 개인 데이터 또는 민감한 데이터에 사용하기 위한 것이 아닙니다.

문제 해결

AWS Transfer Family프로파일에 태그를 추가하는 방법에 대한 자세한 내용은 리소스 태그 지정 및 태그 편집기 사용 설명서의 리소스 태그 지정 방법을 참조하세요. AWS

## 에 대한 Security Hub CSPM 제어AWS WAF

이러한 AWS Security Hub CSPM제어는 AWS WAF서비스 및 리소스를 평가합니다. 컨트롤을 전혀 사용하지 못할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::WAF::WebACL`

AWS Config 규칙: `waf-classic-logging-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 AWS WAF글로벌 웹 ACL에 로깅이 활성화되어 있는지 확인합니다. 웹 ACL에 로깅이 활성화되지 않은 경우, 이 제어는 실패합니다.

로깅은 AWS WAF전 세계의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다. 이는 많은 조직의 비즈니스 및 규정 준수 요구 사항이며, 이를 통해 애플리케이션 동작 문제를 해결할 수 있습니다. 또한 AWS WAF에 연결된 웹 ACL을 통해 분석된 트래픽에 대한 상세 정보도 제공합니다.

문제 해결

AWS WAF웹 ACL에 대한 로깅을 활성화하려면 AWS WAF개발자 안내서의 웹 ACL 트래픽 정보 로깅을 참조하세요.

[WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFRegional::Rule`

AWS Config 규칙: `waf-regional-rule-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAF리전 규칙에 하나 이상의 조건이 있는지 확인합니다. 규칙 내에 조건이 없는 경우, 제어가 실패합니다.

WAF 리전별 규칙에는 여러 조건이 포함될 수 있습니다. 규칙의 조건에 따라 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 아무 조건 없이 트래픽은 검사 없이 통과합니다. 조건은 없지만 허용, 차단 또는 개수를 제안하는 이름이나 태그가 있는 WAF 리전별 규칙은 해당 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

문제 해결

빈 규칙에 조건을 추가하려면 AWS WAF 개발자 안내서의 규칙에서 조건 추가 및 제거를 참조하세요.

[WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFRegional::RuleGroup`

AWS Config 규칙: `waf-regional-rulegroup-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAF리전 규칙 그룹에 하나 이상의 규칙이 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우, 제어가 실패합니다.

WAF 리전별 규칙 그룹에는 여러 규칙이 포함될 수 있습니다. 규칙의 조건에 따라 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 규칙이 없으면 트래픽은 검사 없이 통과합니다. 규칙이 없지만 허용, 차단 또는 개수를 암시하는 이름 또는 태그가 있는 WAF 리전별 규칙 그룹은 이러한 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

문제 해결

빈 규칙 그룹에 규칙 및 규칙 조건을 추가하려면 AWS WAF개발자 안내서의 AWS WAFClassic 규칙 그룹에서 규칙 추가 및 삭제 및 규칙에서 조건 추가 및 제거를 참조하세요.

[WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFRegional::WebACL`

AWS Config 규칙: `waf-regional-webacl-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAF Classic Regional웹 ACL에 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않으면 이 제어가 실패합니다.

WAF 리전별 웹 ACL에는 웹 요청을 검사하고 제어하는 규칙 및 규칙 그룹 모음이 포함될 수 있습니다. 웹 ACL이 비어 있는 경우, 웹 트래픽은 기본 작업에 따라 WAF에 의해 감지되거나 조치되지 않고 통과할 수 있습니다.

문제 해결

빈 AWS WAFClassic 리전 웹 ACL에 규칙 또는 규칙 그룹을 추가하려면 AWS WAF개발자 안내서의 웹 ACL 편집을 참조하세요.

[WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAF::Rule`

AWS Config 규칙: `waf-global-rule-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAF글로벌 규칙에 조건이 포함되어 있는지 확인합니다. 규칙 내에 조건이 없는 경우, 제어가 실패합니다.

WAF 글로벌 규칙은 여러 조건을 포함할 수 있습니다. 규칙의 조건을 통해 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 아무 조건 없이 트래픽은 검사 없이 통과합니다. 규칙은 없지만 허용, 차단 또는 개수를 암시하는 이름이나 태그가 있는 WAF 글로벌 규칙은 해당 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

문제 해결

규칙 생성 및 조건 추가에 대한 지침은 AWS WAF 개발자 안내서의 규칙 생성 및 조건 추가를 참조하세요.

[WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAF::RuleGroup`

AWS Config 규칙: `waf-global-rulegroup-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAF글로벌 규칙 그룹에 하나 이상의 규칙이 있는지 확인합니다. 규칙 그룹 내에 규칙이 없는 경우, 제어가 실패합니다.

WAF 글로벌 규칙 그룹은 여러 규칙을 포함할 수 있습니다. 규칙의 조건에 따라 트래픽을 검사하고 정의된 조치(허용, 차단 또는 계산)를 수행할 수 있습니다. 규칙이 없으면 트래픽은 검사 없이 통과합니다. 규칙은 없지만 허용, 차단 또는 개수를 암시하는 이름이나 태그가 있는 WAF 글로벌 규칙 그룹은 해당 작업 중 하나가 발생하고 있다고 잘못 가정할 수 있습니다.

문제 해결

규칙 그룹에 규칙을 추가하는 방법에 대한 지침은 AWS WAF개발자 안내서의 AWS WAF클래식 규칙 그룹 생성을 참조하세요.

[WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

관련 요구 사항: 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)

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAF::WebACL`

AWS Config 규칙: `waf-global-webacl-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAF글로벌 웹 ACL에 하나 이상의 WAF 규칙 또는 WAF 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 WAF 규칙 또는 규칙 그룹이 포함되어 있지 않으면 제어가 실패합니다.

WAF 글로벌 웹 ACL은 웹 요청을 검사하고 제어하기 위한 규칙 및 규칙 그룹 모음을 포함할 수 있습니다. 웹 ACL이 비어 있는 경우, 웹 트래픽은 기본 작업에 따라 WAF에 의해 감지되거나 조치되지 않고 통과할 수 있습니다.

문제 해결

빈 AWS WAF글로벌 웹 ACL에 규칙 또는 규칙 그룹을 추가하려면 AWS WAF개발자 안내서의 웹 ACL 편집을 참조하세요. 필터에서 글로벌(CloudFront)을 선택합니다.

[WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

관련 요구 사항: NIST.800-53.r5 CA-9(1), NIST.800-53.r5 CM-2

범주: 보호 > 보안 네트워크 구성

심각도: 중간

리소스 유형: `AWS::WAFv2::WebACL`

AWS Config 규칙: `wafv2-webacl-not-empty`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAFV2 웹 액세스 제어 목록(웹 ACL)에 하나 이상의 규칙 또는 규칙 그룹이 포함되어 있는지 확인합니다. 웹 ACL에 규칙 또는 규칙 그룹이 포함되어 있지 않으면 제어가 실패합니다.

웹 ACL을 사용하면 보호된 리소스가 응답하는 모든 HTTP(S) 웹 요청을 세밀하게 제어할 수 있습니다. 웹 ACL에는 웹 요청을 검사하고 제어하기 위한 규칙 및 규칙 그룹 모음이 포함되어야 합니다. 웹 ACL이 비어 있는 경우 기본 작업에 AWS WAF따라가 감지하거나 조치를 취하지 않고 웹 트래픽이 전달될 수 있습니다.

문제 해결

빈 WAFV2 웹 ACL에 규칙 또는 규칙 그룹을 추가하려면 AWS WAF 개발자 안내서의 웹 ACL 편집을 참조하세요.

[WAF.11]AWS WAF웹 ACL 로깅을 활성화해야 합니다.

관련 요구 사항: 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

범주: 식별 > 로깅

심각도: 낮음

리소스 유형: `AWS::WAFv2::WebACL`

AWS Config규칙: `wafv2-logging-enabled`

스케줄 유형: 주기적

파라미터: 없음

이 제어는 로깅이 AWS WAFV2 웹 액세스 제어 목록(웹 ACL)에 대해 활성화되었는지 확인합니다. 웹 ACL에 대한 로깅이 비활성화되면 이 제어가 실패합니다.

> **Note**
>
> 이 제어는 Amazon Security Lake를 통해 계정에 웹 AWS WAFACL 로깅이 활성화되어 있는지 여부를 확인하지 않습니다.

로깅은의 안정성, 가용성 및 성능을 유지합니다AWS WAF. 또한 로깅은 많은 조직의 비즈니스 및 규정 준수 요구 사항입니다. 웹 ACL로 분석된 트래픽을 로깅하여 애플리케이션 동작 문제를 해결할 수 있습니다.

문제 해결

AWS WAF웹 ACL에 대한 로깅을 활성화하려면 AWS WAF개발자 안내서의 웹 ACL에 대한 로깅 관리를 참조하세요.

[WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.

관련 요구 사항: 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), NIST.800-171.r2 3.14.6, NIST.800-171.r2 3.14.7

범주: 식별 > 로깅

심각도: 중간

리소스 유형: `AWS::WAFv2::RuleGroup`

AWS Config규칙: `wafv2-rulegroup-logging-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 AWS WAF규칙 또는 규칙 그룹에 Amazon CloudWatch 지표가 활성화되어 있는지 확인합니다. 규칙 또는 규칙 그룹에 CloudWatch 메트릭이 활성화되어 있지 않으면 제어가 실패합니다.

AWS WAF규칙 및 규칙 그룹에 CloudWatch 지표를 구성하면 트래픽 흐름을 파악할 수 있습니다. 어떤 ACL 규칙이 트리거되고 어떤 요청이 수락 및 차단되었는지 확인할 수 있습니다. 이러한 가시성을 통해 관련 리소스에서 악의적인 활동을 식별할 수 있습니다.

문제 해결

AWS WAF규칙 그룹에서 CloudWatch 지표를 활성화하려면 UpdateRuleGroup API를 호출합니다. AWS WAF규칙에 대해 CloudWatch 지표를 활성화하려면 UpdateWebACL API를 호출합니다. `CloudWatchMetricsEnabled` 필드를 `true`(으)로 설정합니다. AWS WAF콘솔을 사용하여 규칙 또는 규칙 그룹을 생성하면 CloudWatch 지표가 자동으로 활성화됩니다.

## WorkSpaces에 대한 Security Hub CSPM 제어

이러한 AWS Security Hub CSPM제어는 Amazon WorkSpaces 서비스 및 리소스를 평가합니다.

이러한 제어는 일부만 사용할 수 있습니다AWS 리전. 자세한 내용은 리전별 제어 기능 사용 가능 여부 단원을 참조하십시오.

[WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::WorkSpaces::Workspace`

AWS Config 규칙: `workspaces-user-volume-encryption-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon WorkSpaces WorkSpace의 사용자 볼륨이 저장 시 암호화되는지 확인합니다. WorkSpace 사용자 볼륨이 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 저장 데이터를 암호화하면 기밀성을 보호할 수 있으므로 권한이 없는 사용자가 데이터에 액세스할 수 있는 위험이 줄어듭니다.

문제 해결

WorkSpaces 사용자 볼륨을 암호화하려면 Amazon WorkSpaces 관리 안내서의 WorkSpace 암호화를 참조하세요.

[WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

범주: 보호 > 데이터 보호 > 저장 데이터 암호화

심각도: 중간

리소스 유형: `AWS::WorkSpaces::Workspace`

AWS Config 규칙: `workspaces-root-volume-encryption-enabled`

스케줄 유형: 변경이 트리거됨

파라미터: 없음

이 제어는 Amazon WorkSpaces WorkSpace의 루트 볼륨이 저장 시 암호화되는지 확인합니다. WorkSpace 루트 볼륨이 저장 시 암호화되지 않으면 제어가 실패합니다.

저장 데이터는 일정 기간 동안 영구 비휘발성 스토리지에 저장되는 모든 데이터를 의미합니다. 저장 데이터를 암호화하면 기밀성을 보호할 수 있으므로 권한이 없는 사용자가 데이터에 액세스할 수 있는 위험이 줄어듭니다.

문제 해결

WorkSpaces 루트 볼륨을 암호화하려면 Amazon WorkSpaces 관리 안내서의 WorkSpace 암호화를 참조하세요.

## Security Hub CSPM에서 제어를 구성하는 데 필요한 권한

보안 제어에 대한 정보를 보고 표준에서 보안 제어를 활성화 및 비활성화하려면 AWSSecurity Hub CSPM에 액세스하는 데 사용하는 AWS Identity and Access Management(IAM) 역할에 Security Hub CSPM API의 다음 작업을 호출할 권한이 필요합니다.

필요한 권한을 얻으려면 Security Hub CSPM 관리형 정책을 사용할 수 있습니다. 또는 이러한 작업에 대한 권한을 포함하도록 사용자 지정 IAM 정책을 업데이트할 수 있습니다.

- BatchGetSecurityControls - 현재 계정 및의 보안 제어 배치에 대한 정보를 반환합니다AWS 리전.
- ListSecurityControlDefinitions - 지정된 표준에 적용되는 보안 제어에 대한 정보를 반환합니다.
- ListStandardsControlAssociations - 계정에서 활성화된 각 표준에서 보안 제어가 현재 활성화되어 있는지 또는 비활성화되어 있는지 식별합니다.
- BatchGetStandardsControlAssociations - 보안 제어 배치의 경우, 각 제어가 현재 지정된 표준에서 활성화되었는지 또는 비활성화되었는지 식별합니다.
- BatchUpdateStandardsControlAssociations - 제어를 포함하는 표준에서 보안 제어를 활성화하거나 표준에서 제어를 비활성화하는 데 사용됩니다. 이는 기존 `UpdateStandardsControl` 작업을 일괄적으로 대체하는 것입니다.
- BatchUpdateStandardsControlAssociations - 제어를 포함하는 표준에서 보안 제어를 활성화하거나 표준에서 제어를 비활성화하는 데 사용됩니다. 이는 기존 `UpdateStandardsControl` 작업을 일괄적으로 대체하는 것입니다.
- UpdateStandardsControl - 표준에서 제어를 포함하는 보안 제어를 활성화하거나 비활성화하는 데 사용됩니다.
- DescribeStandardsControl - 지정된 보안 제어에 대한 세부 정보를 반환합니다.

위의 API 외에도 IAM 역할에 `BatchGetControlEvaluations`을(를) 호출할 권한을 추가해야 합니다. 이 권한은 Security Hub CSPM 콘솔에서 제어 활성화 및 규정 준수 상태, 제어에 대한 조사 결과 수, 제어에 대한 전체 보안 점수를 보는 데 필요합니다. 콘솔만를 호출하므로 `BatchGetControlEvaluations`이 권한은 공개적으로 문서화된 Security Hub CSPM APIs 또는 AWS CLI명령에 직접 해당하지 않습니다.

## Security Hub CSPM에서 제어 활성화

AWS Security Hub CSPM에서 제어는 조직이 정보의 기밀성, 무결성 및 가용성을 보호하는 데 도움이 되는 보안 표준 내의 보호 장치입니다. 각 Security Hub CSPM 제어는 특정 AWS 리소스와 관련이 있습니다. 표준에서 제어를 활성화하면 Security Hub CSPM이 제어에 대한 보안 검사를 실행하고 제어에

대한 조사 결과를 생성하기 시작합니다. 또한 Security Hub CSPM은 보안 점수를 계산할 때 활성화된 모든 제어를 고려합니다.

적용되는 모든 보안 표준에서 제어를 활성화하도록 선택할 수 있습니다. 또는 여러 표준에서 활성화 상태를 다르게 구성할 수 있습니다. 제어 활성화 및 비활성화를 선택하여 제어의 활성화 상태를 사용 가능한 모든 표준에 맞게 조정하는 것이 좋습니다. 이것이 적용되는 모든 표준에서 제어를 활성화하는 방법에 대한 지침은 표준에서 제어 활성화 섹션을 참조하세요. 모든 표준에서 제어를 활성화하는 방법에 대한 지침은 특정 표준에서 제어 활성화하기 섹션을 참조하세요.

교차 리전 집계를 활성화하고 집계 영역에 로그인하면 Security Hub CSPM 콘솔에는 하나 이상의 연결된 리전에서 사용할 수 있는 제어가 표시됩니다. 연결된 리전에서는 제어를 사용할 수 있지만 집계 영역에서는 사용할 수 없는 경우, 집계 영역에서 해당 제어를 활성화하거나 비활성화할 수 없습니다.

Security Hub CSPM 콘솔, Security Hub CSPM API 또는를 사용하여 각 리전에서 제어를 활성화 및 비활성화할 수 있습니다 AWS CLI.

제어 활성화 및 비활성화 지침은 중앙 구성 사용 여부에 따라 달라집니다. 이 주제에서는 차이점을 설명합니다. Security Hub CSPM 및를 통합하는 사용자는 중앙 구성을 사용할 수 있습니다 AWS Organizations. 다중 계정, 다중 리전 환경에서 제어를 활성화 또는 비활성화하는 프로세스를 단순화하려면 중앙 구성을 사용하는 것이 좋습니다. 중앙 구성을 사용하는 경우, 구성 정책을 사용하여 여러 계정 및 리전에서 제어를 활성화할 수 있습니다. 중앙 구성을 사용하지 않는 경우, 각 계정 및 리전에서 개별적으로 Security Hub를 구성해야 합니다.

## 표준에서 제어 활성화

제어가 적용되는 모든 표준에서 AWS Security Hub CSPM 제어를 활성화하는 것이 좋습니다. 통합 제어 조사 결과를 켜면 제어가 하나 이상의 표준에 속하더라도 제어 검사당 하나의 조사 결과를 받게 됩니다.

다중 계정, 다중 리전 환경에서의 교차 표준 활성화

여러 AWS 계정 및에서 보안 제어를 활성화하려면 위임된 Security Hub CSPM 관리자 계정에 로그인하고 중앙 구성을 사용해야 AWS 리전합니다.

중앙 구성을 사용하는 경우, 위임된 관리자는 사용 가능한 표준에 대해 지정된 제어를 활성화하는 Security Hub CSPM 구성 정책을 만들 수 있습니다. 그런 다음 구성 정책을 특정 계정 및 OU(조직 단위) 또는 루트와 연결할 수 있습니다. 구성 정책은 홈 리전(집계 리전이라고도 함) 및 연결된 모든 리전에 적용됩니다.

구성 정책은 사용자 지정을 제공합니다. 예를 들어, 한 OU에서는 모든 제어를 활성화하고 다른 OU에서는 Amazon Elastic Compute Cloud(EC2) 제어만 활성화하도록 선택할 수 있습니다. 세분화 수준은

조직의 보안 범위에 대한 의도한 목표에 따라 달라집니다. 표준 전반에 걸쳐 지정된 제어를 활성화하는 구성 정책을 만드는 방법에 대한 지침은 구성 정책 생성 및 연결 섹션을 참조하세요.

> **Note**
>
> 위임된 관리자는 서비스 관리형 표준을 제외한 모든 표준에서 제어를 관리하는 구성 정책을 생성할 수 있습니다 AWS Control Tower. 이 표준에 대한 제어는 AWS Control Tower 서비스에서 구성해야 합니다.

일부 계정에서 위임된 관리자가 아닌 자체 제어를 구성하도록 하려면 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 개별적으로 제어를 구성해야 합니다.

단일 계정 및 리전에서 표준 간 활성화

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우, 구성 정책을 사용하여 다중 계정 및 리전에서 제어를 중앙에서 활성화할 수 없습니다. 하지만 다음 단계를 사용하여 단일 계정 및 리전에서 제어를 활성화할 수 있습니다.

Security Hub CSPM console

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다.
3. 비활성화 탭을 선택합니다.
4. 제어 옆에 있는 옵션을 선택합니다.
5. 제어 활성화를 선택합니다(이 옵션은 이미 활성화된 제어에는 표시되지 않습니다).
6. 제어를 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

Security Hub CSPM API

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 활성화하려면

1. ListStandardsControlAssociations API를 호출합니다. 보안 제어 ID를 제공합니다.

   요청 예제:

```
{
    "SecurityControlId": "IAM.1"
}
```

2. BatchUpdateStandardsControlAssociations API를 호출합니다. 제어가 활성화되지 않은 표준의 Amazon 리소스 이름(ARN)을 제공합니다. 표준 ARN을 가져오려면 DescribeStandards을(를) 실행하세요.
3. AssociationStatus 파라미터를 ENABLED와(과) 동일하게 설정합니다. 이미 활성화된 제어에 대해 다음 단계를 수행하면 API가 HTTP 상태 코드 200 응답을 반환합니다.

   요청 예제:

```
{
    "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. 제어를 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

AWS CLI

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 활성화하려면

1. list-standards-control-associations 명령을 실행합니다. 보안 제어 ID를 제공합니다.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. batch-update-standards-control-associations 명령을 실행합니다. 제어가 활성화되지 않은 표준의 Amazon 리소스 이름(ARN)을 제공합니다. 표준 ARN을 얻으려면 describe-standards 명령을 실행합니다.
3. AssociationStatus 파라미터를 ENABLED와(과) 동일하게 설정합니다. 이미 활성화된 제어에 대해 다음 단계를 수행하면 명령은 HTTP 상태 코드 200 응답을 반환합니다.

```
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. 제어를 활성화하려는 각 리전에 대해 이 단계를 반복합니다.

## 특정 표준에서 제어 활성화하기

AWS Security Hub CSPM에서 표준을 활성화하면 해당 표준에 적용되는 모든 제어가 해당 표준에서 자동으로 활성화됩니다(이에 대한 예외는 서비스 관리형 표준). 그런 다음 표준 내에서 특정 제어를 비활성화하고 다시 활성화할 수 있습니다. 하지만 제어의 활성화 상태를 활성화된 모든 표준에 맞게 조정하는 것이 좋습니다. 모든 표준에서 제어를 활성화하는 방법에 대한 지침은 표준에서 제어 활성화 섹션을 참조하세요.

표준의 세부 정보 페이지에는 표준에 적용할 수 있는 제어 목록과 해당 표준에서 현재 활성화되고 비활성화된 제어에 대한 정보가 포함되어 있습니다.

또한 표준 세부 정보 페이지에서 특정 표준의 제어를 활성화할 수도 있습니다. 각 AWS 계정 및에서 특정 표준의 제어를 개별적으로 활성화해야 합니다 AWS 리전. 특정 표준에서 제어를 활성화하면 현재 계정 및 리전에만 영향을 미칩니다.

표준에서 제어를 활성화하려면 먼저 제어가 적용되는 표준을 하나 이상 활성화해야 합니다. 표준을 활성화하는 방법에 대한 지침은 보안 표준 활성화 섹션을 참조하세요. 하나 이상의 표준에서 제어를 활성화하면 Security Hub CSPM은 해당 제어에 대한 조사 결과를 생성하기 시작합니다. Security Hub CSPM은 전체 보안 점수 및 표준 보안 점수 계산에 제어 상태를 포함합니다. 여러 표준에서 제어를 활성화하더라도 통합 제어 조사 결과를 켜면 표준 전반에 걸쳐 보안 검사당 단일 조사 결과를 받게 됩니다. 자세한 내용은 통합 제어 조사 결과를 참조하세요.

표준에서 제어를 활성화하려면 현재 리전에서 제어를 사용할 수 있어야 합니다. 자세한 내용은 리전별 제어 가용성 섹션을 참조하세요.

다음 단계에 따라 특정 표준에서 Security Hub CSPM 제어를 활성화합니다. 다음 단계 대신 `UpdateStandardsControl` API 작업을 사용하여 특정 표준에서 제어를 활성화할 수도 있습니다. 모든 표준에서 제어를 활성화하는 방법에 대한 지침은 단일 계정 및 리전에서 표준 간 활성화 섹션을 참조하세요.

Security Hub CSPM console

특정 표준에서 제어를 활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 보안 표준을 선택합니다.
3. 관련 표준의 결과 보기를 선택합니다.
4. 제어를 선택합니다.
5. 제어 활성화를 선택합니다(이 옵션은 이미 활성화된 제어에는 표시되지 않습니다). 활성화를 선택하여 확인합니다.

Security Hub CSPM API

특정 표준에서 제어를 활성화하려면

1. ListSecurityControlDefinitions을(를) 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 DescribeStandards을(를) 실행하세요. 이 API는 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

   요청 예제:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations을(를) 실행하고 특정 제어 ID를 입력하여 각 표준에서 제어의 현재 활성화 상태를 반환하세요.

   요청 예제:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. BatchUpdateStandardsControlAssociations을(를) 실행합니다. 제어를 활성화하려는 표준의 ARN을 입력합니다.
4. `AssociationStatus` 파라미터를 `ENABLED`와(과) 동일하게 설정합니다.

요청 예제:

```
{
    "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
 "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

특정 표준에서 제어를 활성화하려면

1. list-security-control-definitions 명령을 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 describe-standards을(를) 실행하세요. 이 명령은 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

```
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. list-standards-control-associations 명령을 실행하고 특정 제어 ID를 제공하여 각 표준에서 제어의 현재 활성화 상태를 반환합니다.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations 명령을 실행합니다. 제어를 활성화하려는 표준의 ARN을 입력합니다.
4. AssociationStatus 파라미터를 ENABLED와(과) 동일하게 설정합니다.

```
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"}]'
```

## 활성화된 표준에서 자동으로 새로운 제어 활성화

AWSSecurity Hub CSPM은 정기적으로 새 컨트롤을 릴리스하고 하나 이상의 표준에 추가합니다. 활성화된 표준에서 새로운 제어를 자동으로 활성화할 것인지를 선택할 수 있습니다.

새로운 보안 제어를 자동으로 활성화하려면 Security Hub CSPM 중앙 구성을 사용하는 것이 좋습니다. 표준 전반에 걸쳐 비활성화할 제어 목록을 포함하는 구성 정책을 만들 수 있습니다. 새롭게 릴리스된 제어를 포함한 다른 모든 제어는 기본적으로 활성화됩니다. 또는 표준 전반에 걸쳐 활성화할 제어 목록을 포함하는 정책을 만들 수 있습니다. 새롭게 릴리스된 제어를 포함한 다른 모든 제어는 기본적으로 비활성화됩니다. 자세한 내용은 Security Hub CSPM의 중앙 구성 이해 단원을 참조하십시오.

활성화하지 않은 표준에 새로운 제어를 추가하면 Security Hub CSPM에서 새로운 제어가 활성화되지 않습니다.

다음 지침은 중앙 구성을 사용하지 않는 경우에만 적용됩니다.

원하는 액세스 방법을 선택하고 단계에 따라 활성화된 표준에서 새로운 제어를 자동으로 활성화하는 단계를 따릅니다.

> **Note**
>
> 다음 지침을 사용하여 새 제어를 자동으로 활성화하면 릴리스 직후 콘솔에서 또는 프로그래밍 방식으로 제어와 상호 작용할 수 있습니다. 하지만 자동으로 활성화된 제어의 임시 기본 상태는 비활성화됨입니다. Security Hub CSPM이 제어 릴리스를 처리하고 계정에서 제어를 활성화됨으로 지정하는 데 최대 며칠이 걸릴 수 있습니다. 이 처리 기간 도중에 제어를 수동으로 활성화하거나 비활성화할 수 있으며, Security Hub CSPM은 자동 제어 활성화가 켜져 있는지 여부에 관계없이 해당 지정을 유지합니다.

Security Hub CSPM console

새로운 제어를 자동으로 활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 일반 탭을 선택합니다.
3. 제어에서 편집을 선택합니다.
4. 활성화된 표준에서 새로운 제어 자동 활성화를 켜세요.
5. 저장을 선택합니다.

Security Hub CSPM API

새로운 제어를 자동으로 활성화하려면

1. UpdateSecurityHubConfiguration을(를) 실행합니다.
2. 활성화된 표준에 대해 새로운 제어를 자동으로 활성화하려면 AutoEnableControls을(를) true(으)로 설정합니다. 새로운 제어를 자동으로 활성화하지 않으려면 AutoEnableControls을(를) false로 설정합니다.

AWS CLI

새로운 제어를 자동으로 활성화하려면

1. update-security-hub-configuration 명령을 실행합니다.
2. 활성화된 표준에 대해 새로운 제어를 자동으로 활성화하려면 --auto-enable-controls을(를) 지정합니다. 새로운 제어를 자동으로 활성화하지 않으려면 --no-auto-enable-controls을(를) 지정합니다.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

명령 예제:

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

새로운 제어를 자동으로 활성화하지 않는 경우, 수동으로 활성화해야 합니다. 지침은 Security Hub CSPM에서 제어 활성화 섹션을 참조하세요.

## Security Hub CSPM에서 제어 비활성화

조사 결과 노이즈를 줄이려면 환경과 관련이 없는 제어를 비활성화하는 것이 도움이 될 수 있습니다. AWS Security Hub CSPM에서는 모든 보안 표준에서 또는 특정 표준에 대해서만 제어를 비활성화할 수 있습니다.

모든 표준에서 제어를 비활성화하면 다음과 같은 결과가 발생합니다.

- 해당 제어에 대한 보안 검사가 더 이상 수행되지 않습니다.
- 해당 제어에 대해 추가 조사 결과가 생성되지 않습니다.

- 해당 제어에 대한 기존 조사 결과가 더 이상 업데이트되지 않습니다.
- 기존 조사 결과는 일반적으로 BEB(best-effort basis) 방식으로 3~5일 이내에 자동으로 보관됩니다.
- Security Hub CSPM은 제어를 위해 생성한 모든 관련 AWS Config 규칙을 제거합니다.

특정 표준에서만 제어를 비활성화하면 Security Hub CSPM은 해당 표준에서만 제어에 대한 보안 검사 실행을 중지합니다. 또한 각 표준의 보안 점수 계산에서 해당 제어가 제거됩니다. 해당 제어가 다른 표준에서 활성화되어 있는 경우 Security Hub CSPM은 해당하는 경우 관련 AWS Config 규칙을 유지하고 다른 표준에서는 해당 제어에 대한 보안 검사를 계속 실행합니다. Security Hub CSPM이 다른 각 표준에 대한 보안 점수를 계산할 때에 해당 제어도 포함하며, 이는 요약 보안 점수에 영향을 미칩니다.

표준을 비활성화하면 해당 표준에 적용되는 모든 제어가 자동으로 비활성화됩니다. 하지만 다른 표준에서는 제어가 계속 활성화될 수 있습니다. 표준을 비활성화하면 Security Hub CSPM은 해당 표준에서 어떤 제어가 비활성화되었는지 추적하지 않습니다. 이후에 표준을 다시 활성화하면 해당 표준에 적용되는 모든 제어가 자동으로 활성화됩니다. 표준 비활성화에 대한 자세한 내용은 표준 비활성화을 참조하십시오.

제어 비활성화는 영구적인 작업이 아닙니다. 제어를 비활성화한 다음 해당 제어가 포함된 표준을 활성화한다고 가정해 보겠습니다. 그러면 해당 제어가 이 표준에 대해 활성화됩니다. Security Hub CSPM에서 표준을 활성화하면 해당 표준에 적용되는 모든 제어가 자동으로 활성화됩니다. 표준 활성화에 대한 자세한 내용은 표준 활성화 섹션을 참조하세요.

주제

- 표준에서 제어 비활성화
- 특정 표준의 제어 비활성화
- Security Hub CSPM에서 비활성화가 권장되는 제어

## 표준에서 제어 비활성화

조직 전체에서 일관성을 유지하려면 표준 전반에 걸쳐 AWS Security Hub CSPM 제어를 비활성화하는 것이 좋습니다. 특정 표준에서만 제어를 비활성화하면 다른 표준에서 활성화된 경우 해당 제어에 대한 조사 결과를 계속 수신할 수 있습니다.

여러 계정 및 리전의 표준 간 비활성화

여러 AWS 계정 및에서 보안 제어를 비활성화하려면 중앙 구성을 사용해야 AWS 리전합니다.

중앙 구성을 사용하는 경우, 위임된 관리자는 사용 가능한 표준에 대해 지정된 제어를 비활성화하는 Security Hub CSPM 구성 정책을 만들 수 있습니다. 그런 다음 구성 정책을 특정 계정, OU 또는 루트와 연결할 수 있습니다. 구성 정책은 홈 리전(집계 영역이라고도 함) 및 연결된 모든 리전에 적용됩니다.

구성 정책은 사용자 지정을 제공합니다. 예를 들어 한 OU에서 모든 AWS CloudTrail 제어를 비활성화하도록 선택하고 다른 OU에서 모든 IAM 제어를 비활성화하도록 선택할 수 있습니다. 세분화 수준은 조직의 보안 범위에 대한 의도한 목표에 따라 달라집니다. 표준 전반에 걸쳐 지정된 제어를 비활성화하는 구성 정책을 만드는 방법에 대한 지침은 구성 정책 생성 및 연결 섹션을 참조하세요.

> **Note**
>
> 위임된 관리자는 서비스 관리형 표준을 제외한 모든 표준에서 제어를 관리하는 구성 정책을 생성할 수 있습니다 AWS Control Tower. 이 표준에 대한 제어는 AWS Control Tower 서비스에서 구성해야 합니다.

일부 계정에서 위임된 관리자가 아닌 자체 제어를 구성하도록 하려면 위임된 관리자가 해당 계정을 자체 관리형 계정으로 지정할 수 있습니다. 자체 관리형 계정은 각 리전에서 개별적으로 제어를 구성해야 합니다.

단일 계정 및 리전에서 표준 간 비활성화

중앙 구성을 사용하지 않거나 자체 관리형 계정인 경우, 구성 정책을 사용하여 다중 계정 및 리전에서 제어를 중앙에서 비활성화할 수 없습니다. 하지만 단일 계정 및 리전에서는 제어를 비활성화할 수 있습니다.

Security Hub CSPM console

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다.
3. 제어 옆에 있는 옵션을 선택합니다.
4. 제어 비활성화를 선택합니다. 이미 비활성화된 제어에는 이 옵션이 나타나지 않습니다.
5. 제어를 비활성화하는 이유를 선택하고 비활성화를 선택하여 확인합니다.
6. 제어를 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

### Security Hub CSPM API

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 비활성화하려면

1. ListStandardsControlAssociations API를 호출합니다. 보안 제어 ID를 제공합니다.

   요청 예제:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

2. BatchUpdateStandardsControlAssociations API를 호출합니다. 제어가 활성화된 모든 표준의 ARN을 입력합니다. 표준 ARN을 가져오려면 `DescribeStandards`을(를) 실행하세요.
3. `AssociationStatus` 파라미터를 `DISABLED`와(과) 동일하게 설정합니다. 이미 비활성화된 제어에 대해 다음 단계를 수행하면 API가 HTTP 상태 코드 200 응답을 반환합니다.

   요청 예제:

   ```
   {
       "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. 제어를 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

### AWS CLI

한 계정 및 리전에서 표준 전반에 걸쳐 제어를 비활성화하려면

1. list-standards-control-associations 명령을 실행합니다. 보안 제어 ID를 제공합니다.

   ```
   aws securityhub  --region us-east-1 list-standards-control-associations --
   security-control-id CloudTrail.1
   ```

2. batch-update-standards-control-associations 명령을 실행합니다. 제어가 활성화된 모든 표준의 ARN을 입력합니다. 표준 ARN을 얻으려면 `describe-standards` 명령을 실행합니다.
3. `AssociationStatus` 파라미터를 `DISABLED`와(과) 동일하게 설정합니다. 이미 비활성화된 제어에 대해 다음 단계를 수행하면 명령이 HTTP 상태 코드 200 응답을 반환합니다.

```
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. 제어를 비활성화하려는 각 리전에 대해 이 단계를 반복합니다.

## 특정 표준의 제어 비활성화

모든 보안 표준이 아닌 특정 보안 표준에서만 제어를 비활성화할 수 있습니다. 제어가 활성화된 다른 표준에 적용되는 경우 AWS Security Hub CSPM은 제어에 대한 보안 검사를 계속 실행하고 사용자는 제어에 대한 조사 결과를 계속 수신합니다.

제어의 활성화 상태를 제어가 적용되는 모든 활성화된 표준에 맞게 조정하는 것이 좋습니다. 적용되는 모든 표준에서 제어를 비활성화하는 방법에 대한 자세한 내용은 표준에서 제어 비활성화 섹션을 참조하세요.

표준 세부 정보 페이지에서 특정 표준의 제어를 활성화하고 비활성화할 수도 있습니다. 각 AWS 계정 및에서 특정 표준의 제어를 개별적으로 비활성화해야 합니다 AWS 리전. 특정 표준에서 제어를 비활성화하면 현재 계정 및 리전에만 영향을 미칩니다.

원하는 방법을 선택하고 다음 단계에 따라 하나 이상의 특정 표준에서 제어를 비활성화합니다.

Security Hub CSPM console

특정 표준에서 제어를 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 보안 표준을 선택합니다. 관련 표준의 결과 보기를 선택합니다.
3. 제어를 선택합니다.

4. 제어 비활성화를 선택합니다. 이미 비활성화된 제어에는 이 옵션이 나타나지 않습니다.
5. 제어를 비활성화하는 이유를 제공하고 비활성화를 선택하여 확인합니다.

### Security Hub CSPM API

특정 표준에서 제어를 비활성화하려면

1. ListSecurityControlDefinitions을(를) 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 DescribeStandards을(를) 실행하세요. 이 API는 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

   요청 예제:

   ```
   {
       "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
   }
   ```

2. ListStandardsControlAssociations을(를) 실행하고 특정 제어 ID를 입력하여 각 표준에서 제어의 현재 활성화 상태를 반환하세요.

   요청 예제:

   ```
   {
       "SecurityControlId": "IAM.1"
   }
   ```

3. BatchUpdateStandardsControlAssociations을(를) 실행합니다. 제어를 비활성화하려는 표준의 ARN을 제공합니다.
4. AssociationStatus 파라미터를 DISABLED와(과) 동일하게 설정합니다. 이미 비활성화된 제어에 대해 다음 단계를 수행하면 API가 HTTP 상태 코드 200 응답을 반환합니다.

   요청 예제:

   ```
   {
       "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

특정 표준에서 제어를 비활성화하려면

1. list-security-control-definitions 명령을 실행하고 표준 ARN을 입력하여 특정 표준에 사용할 수 있는 제어 목록을 가져옵니다. 표준 ARN을 얻으려면 describe-standards을(를) 실행하세요. 이 명령은 표준별 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

```
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. list-standards-control-associations 명령을 실행하고 특정 제어 ID를 제공하여 각 표준에서 제어의 현재 활성화 상태를 반환합니다.

```
aws securityhub  --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. batch-update-standards-control-associations 명령을 실행합니다. 제어를 비활성화하려는 표준의 ARN을 제공합니다.
4. AssociationStatus 파라미터를 DISABLED와(과) 동일하게 설정합니다. 이미 활성화된 제어에 대해 다음 단계를 수행하면 명령은 HTTP 상태 코드 200 응답을 반환합니다.

```
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"}]'
```

## Security Hub CSPM에서 비활성화가 권장되는 제어

결과 노이즈 및 사용 비용을 줄이려면 일부 AWSSecurity Hub CSPM 제어를 비활성화하는 것이 좋습니다.

### 글로벌 리소스를 사용하는 제어

일부는 글로벌 리소스를 AWS 서비스지원하므로 모든에서 리소스에 액세스할 수 있습니다AWS 리전. 비용을 절감하기 위해 한 리전을 제외한 모든 리전에서 글로벌 리소스 기록을 비활성화AWS Config할 수 있습니다. 이렇게 한 후에도 Security Hub CSPM은 제어가 활성화된 모든 리전에서 보안 검사를 계속 실행하고 리전별 계정당 검사 횟수에 따라 요금을 부과합니다. 따라서 조사 결과 노이즈를 줄이고 Security Hub CSPM 비용을 절약하려면 글로벌 리소스를 기록하는 리전을 제외한 모든 리전에서 글로벌 리소스와 관련된 다음 제어도 비활성화해야 합니다.

제어에 글로벌 리소스가 포함되어 있지만 한 리전에서만 사용할 수 있는 경우, 해당 리전에서 해당 제어를 비활성화하면 기본 리소스에 대한 조사 결과를 가져올 수 없습니다. 이 경우, 제어를 활성화 상태로 유지하는 것이 좋습니다. 교차 리전 집계를 사용하는 경우, 제어를 사용할 수 있는 리전은 집계 영역 또는 연결된 리전 중 하나여야 합니다. 다음 제어는 글로벌 리소스에 적용되지만 단일 리전에서만 사용할 수 있습니다.

- 모든 CloudFront 제어 - 미국 동부(버지니아 북부) 리전에서만 사용 가능
- GlobalAccelerator.1 – 미국 서부(오리건) 리전에서만 사용 가능
- Route53.2: 미국 동부(버지니아 북부) 리전에서만 사용 가능
- WAF.1, WAF.6, WAF.7 및 WAF.8 - 미국 동부(버지니아 북부) 리전에서만 사용 가능

> **Note**
>
> 중앙 구성을 사용하는 경우, Security Hub CSPM은 홈 리전을 제외한 모든 리전의 글로벌 리소스와 관련된 제어를 자동으로 비활성화합니다. 구성 정책을 통해 활성화하도록 선택한 다른 제어는 사용 가능한 모든 리전에서 활성화됩니다. 이러한 제어에 대한 조사 결과를 한 리전으로만 제한하려면 홈 리전을 제외한 모든 리전에서 AWS Config레코더 설정을 업데이트하고 글로벌 리소스 기록을 끌 수 있습니다.
>
> 글로벌 리소스를 평가하는 활성화된 제어가 홈 리전에서 지원되지 않는 경우 Security Hub CSPM은 해당 제어가 지원되는 연결된 리전에서 제어를 활성화하려고 시도합니다. 중앙 구성을 사용하는 경우, 홈 리전 또는 연결된 리전에서 사용할 수 없는 제어에 대한 적용 범위가 부족합니다.
>
> 중앙 구성에 대한 자세한 내용은 Security Hub CSPM의 중앙 구성 이해 섹션을 참조하세요.

주기적 일정 유형의 제어의 경우, 청구를 방지하려면 Security Hub CSPM에서 이를 비활성화해야 합니다. AWS Config파라미터를 `includeGlobalResourceTypes`로 설정`false`해도 주기적 Security Hub CSPM 제어에는 영향을 주지 않습니다.

다음 Security Hub CSPM 제어는 글로벌 리소스를 사용합니다.

- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.

- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

CloudTrail 로깅 제어

CloudTrail.2 제어는 AWS Key Management Service(AWS KMS)를 사용하여 AWS CloudTrail추적 로그를 암호화합니다. 중앙 집중식 로깅 계정에 이러한 추적을 기록하는 경우 중앙 집중식 로깅이 수행되는 계정 및 AWS 리전위치에서만이 제어를 활성화해야 합니다.

중앙 구성을 사용하는 경우, 제어의 활성화 상태를 홈 리전 및 연결된 리전 전체에 걸쳐 조정합니다. 일부 리전에서는 제어를 비활성화하고 다른 리전에서는 활성화할 수 없습니다. 이 경우, CloudTrail.2 제어에서 조사 결과를 억제하도록 하여 조사 결과 노이즈를 줄일 수 있습니다.

CloudWatch 경보 제어

이상 탐지에 Amazon CloudWatch 경보 대신 Amazon GuardDuty를 사용하려는 경우, CloudWatch 경보에 초점을 맞춘 다음 제어를 비활성화할 수 있습니다.

- [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다.
- [CloudWatch.2] 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.3] MFA 없는 로그인에 대해 관리 콘솔에 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다
- [CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인
- [CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다.
- [CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인
- [CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.
- [CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다.

## Security Hub CSPM의 보안 검사 및 점수 이해

활성화하는 각 제어에 대해 AWSSecurity Hub CSPM은 보안 검사를 실행합니다. 보안 검사는 특정 AWS리소스가 제어에 포함된 규칙을 준수하는지 여부를 알려주는 결과를 생성합니다.

일부 검사는 주기적 일정에 따라 실행됩니다. 리소스 상태가 변경될 때만 실행되는 검사도 있습니다. 자세한 내용은 보안 검사 실행 예약 단원을 참조하십시오.

많은 보안 검사는 AWS Config관리형 또는 사용자 지정 규칙을 사용하여 규정 준수 요구 사항을 설정합니다. 이러한 검사를 실행하려면 필요한 리소스에 대한 리소스 기록을 설정하고 AWS Config활성화해야 합니다. 설정에 대한 자세한 내용은 단원을 AWS Config참조하십시오Security Hub CSPM AWS Config 에 대한 활성화 및 구성. 각 표준에 대해 기록해야 하는 AWS Config리소스 목록은 섹션을 참조하세요제어 조사 결과에 필요한 AWS Config리소스. 다른 제어는 Security Hub CSPM이 관리하고 사전 조건이 필요하지 않은 사용자 지정 Lambda 함수를 사용합니다.

Security Hub CSPM은 보안 검사를 실행할 때 조사 결과를 생성하고 규정 준수 상태를 할당합니다. 규정 준수 상태에 대한 자세한 내용은 Security Hub CSPM 조사 결과의 규정 준수 상태 평가 섹션을 참조하세요.

Security Hub CSPM은 제어 조사 결과의 규정 준수 상태를 사용하여 전체 제어 상태를 결정합니다. 또한 제어 상태에 따라, Security Hub CSPM은 활성화된 모든 제어와 특정 표준에 대한 보안 점수를 계산합니다. 자세한 내용은 the section called “규정 준수 상태 및 제어 상태” 및 the section called “보안 점수 계산” 섹션을 참조하세요.

통합 제어 조사 결과를 활성화한 경우, Security Hub CSPM은 제어가 둘 이상의 표준과 연결된 경우에도 단일 조사 결과를 생성합니다. 자세한 내용은 통합 제어 조사 결과 단원을 참조하십시오.

주제

- 제어 조사 결과에 필요한 AWS Config리소스
- 보안 검사 실행 예약
- 제어 조사 결과 생성 및 업데이트
- 규정 준수 상태 및 제어 상태 평가
- 보안 점수 계산

## 제어 조사 결과에 필요한 AWS Config리소스

> **Note**
>
> Security Hub CSPM 및 Security Hub를 사용하는 경우 리소스 기록의 구성이 관리됩니다. Security Hub는를 사용하여 서비스 연결 구성 레코더를 생성하고 Security Hub CSPM에서 지원되는 제어AWS Config와 관련된 모든 리소스에 대한 직접 정보를 가져옵니다. 자세한 내용은 서비스 연결 구성 레코더 사용 단원을 참조하십시오.

AWSSecurity Hub CSPM에서 일부 제어는 AWS리소스의 구성 변경을 감지하는 서비스 연결 AWS Config규칙을 사용합니다. Security Hub CSPM이 이러한 제어에 대한 정확한 결과를 생성하려면 리소스 기록을 활성화AWS Config하고 활성화해야 합니다AWS Config. Security Hub CSPM이 AWS Config규칙을 사용하는 방법과 활성화 및 구성하는 방법에 대한 자세한 내용은 섹션을 AWS Config참조하세요Security Hub CSPM AWS Config 에 대한 활성화 및 구성. 리소스 기록에 대한 자세한 내용은 AWS Config 개발자 안내서의 구성 레코더 작업을 참조하세요.

정확한 제어 조사 결과를 수신하려면 변경 트리거된 일정 유형으로 활성화된 제어에 대한 AWS Config 리소스 기록을 켜야 합니다. 일정 유형이 주기적인 일부 제어에도 리소스 기록이 필요합니다. 이 페이지에는 이러한 Security Hub CSPM 제어에 필요한 리소스가 나열되어 있습니다.

Security Hub CSPM 제어는 관리형 AWS Config규칙 또는 사용자 지정 Security Hub CSPM 규칙에 의존할 수 있습니다. 가 리소스를 기록할 수 있는 권한을 AWS Config갖지 못하게 하는 AWS Identity and Access Management(IAM) 정책 또는 AWS Organizations관리형 정책이 없는지 확인합니다. Security Hub CSPM 제어는 리소스 구성을 직접 평가하고 AWS Organizations정책을 고려하지 않습니다.

> **Note**
>
> 제어를 사용할 수 없는 AWS 리전에서는 해당 리소스를 사용할 수 없습니다AWS Config. 이러한 한도의 목록은 Security Hub CSPM 제어에 대한 리전별 제한 섹션을 참조하세요.

주제


- 모든 Security Hub CSPM 제어에 필요한 리소스
- AWS기본 보안 모범 사례 표준에 필요한 리소스
- CIS AWS파운데이션 벤치마크에 필요한 리소스
- NIST SP 800-53 개정 5 표준에 필요한 리소스
- NIST SP 800-171 개정 2 표준에 필요한 리소스
- PCI DSS v3.2.1에 필요한 리소스
- 리소스 태그 지정 표준에 필요한 AWS리소스


## 모든 Security Hub CSPM 제어에 필요한 리소스

Security Hub CSPM이 활성화된 변경 트리거 제어에 대한 결과를 생성하고 AWS Config규칙을 사용하려면 다음 유형의 리소스를에 기록해야 합니다AWS Config. 또한 이 테이블에는 특정 유형의 리소스를 제어하는 제어도 나와 있습니다. 단일 제어가 2개 이상의 리소스 유형을 평가할 수 있습니다.

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| AWS Amplify | `AWS::Amplify::App` | Amplify.1 |
| | `AWS::Amplify::Branch` | Amplify.2 |
| Amazon API Gateway | `AWS::ApiGateway::Stage` | APIGateway.1<br>APIGateway.2<br>APIGateway.3<br>APIGateway.4<br>APIGateway.5 |
| | `AWS::ApiGatewayV2::Stage` | APIGateway.1<br>APIGateway.9 |
| | `AWS::ApiGateway::DomainName` | APIGateway.11 |
| AWS AppConfig | `AWS::AppConfig::Application` | AppConfig.1 |
| | `AWS::AppConfig::ConfigurationProfile` | AppConfig.2 |
| | `AWS::AppConfig::Environment` | AppConfig.3 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `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<br>AppSync.4<br>AppSync.5 |
| | `AWS::AppSync::ApiCache` | AppSync.1<br>AppSync.6 |
| AWS Backup | `AWS::Backup::BackupPlan` | Backup.5 |
| | `AWS::Backup::BackupVault` | Backup.3 |
| | `AWS::Backup::RecoveryPoint` | Backup.1<br>Backup.2 |
| | `AWS::Backup::ReportPlan` | Backup.4 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| AWS Batch | `AWS::Batch::ComputeEnvironment` | Batch.3<br>Batch.4 |
| | `AWS::Batch::JobQueue` | Batch.1 |
| | `AWS::Batch::SchedulingPolicy` | Batch.2 |
| Amazon Bedrock | `AWS::Bedrock::DataSource` | Bedrock.1 |
| Amazon Bedrock AgentCore | `AWS::BedrockAgentCore::BrowserCustom` | BedrockAgentCore.5<br>BedrockAgentCore.6 |
| | `AWS::BedrockAgentCore::CodeInterpreterCustom` | BedrockAgentCore.7 |
| | `AWS::BedrockAgentCore::Gateway` | BedrockAgentCore.2<br>BedrockAgentCore.4 |
| | `AWS::BedrockAgentCore::Memory` | BedrockAgentCore.3 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::BedrockAgentCore::Runtime` | BedrockAgentCore.1 |
| AWS Certificate Manager(ACM) | `AWS::ACM::Certificate` | ACM.1<br>ACM.2<br>ACM.3 |
| Amazon Athena | `AWS::Athena::DataCatalog` | Athena.2 |
| | `AWS::Athena::WorkGroup` | Athena.3<br>Athena.4 |
| AWS CloudFormation | `AWS::CloudFormation::Stack` | CloudFormation.2<br>CloudFormation.3<br>CloudFormation.4 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| Amazon CloudFront | `AWS::CloudFront::Distribution` | CloudFront.1<br>CloudFront.3<br>CloudFront.4<br>CloudFront.5<br>CloudFront.6<br>CloudFront.7<br>CloudFront.8<br>CloudFront.9<br>CloudFront.10<br>CloudFront.13<br>CloudFront.14<br>CloudFront.15<br>CloudFront.16<br>CloudFront.17 |
| AWS CloudTrail | `AWS::CloudTrail::Trail` | CloudTrail.9 |
| | `AWS::CloudTrail::EventDataStore` | CloudTrail.11 |
| Amazon CloudWatch | `AWS::CloudWatch::Alarm` | CloudWatch.15<br>CloudWatch.17 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| AWS CodeArtifact | `AWS::CodeArtifact::Repository` | CodeArtifact.1 |
| AWS CodeBuild | `AWS::CodeBuild::Project` | CodeBuild.1<br>CodeBuild.2<br>CodeBuild.3<br>CodeBuild.4 |
| | `AWS::CodeBuild::ReportGroup` | CodeBuild.7 |
| Amazon CodeGuru Profiler | `AWS::CodeGuruProfiler::ProfilingGroup` | CodeGuruProfiler.1 |
| Amazon CodeGuru Reviewer | `AWS::CodeGuruReviewer::RepositoryAssociation` | CodeGuruReviewer.1 |
| Amazon Cognito | `AWS::Cognito::IdentityPool` | Cognito.2 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::Cognito::UserPool` | Cognito.1<br>Cognito.3<br>Cognito.4<br>Cognito.5<br>Cognito.6 |
| Amazon Connect Customer | `AWS::CustomerProfiles::ObjectType` | Connect.1 |
| | `AWS::Connect::Instance` | Connect.2 |
| AWS DataSync | `AWS::DataSync::Task` | DataSync.1<br>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<br>DMS.10<br>DMS.11<br>DMS.12 |
| | `AWS::DMS::EventSubscription` | DMS.3 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::DMS::ReplicationInstance | DMS.4<br>DMS.6<br>DMS.13 |
| | AWS::DMS::ReplicationSubnetGroup | DMS.5 |
| | AWS::DMS::ReplicationTask | DMS.7<br>DMS.8 |
| Amazon DynamoDB | AWS::DynamoDB::Table | DynamoDB.1<br>DynamoDB.2<br>DynamoDB.5<br>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<br>EC2.37 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::EC2::FlowLog | EC2.48 |
| | AWS::EC2::Instance | EC2.4<br>EC2.8<br>EC2.9<br>EC2.17<br>EC2.24<br>EC2.38<br>EMR.1<br>SSM.1 |
| | AWS::EC2::InternetGateway | EC2.39 |
| | AWS::EC2::LaunchTemplate | EC2.25<br>EC2.170<br>EC2.175<br>EC2.181 |
| | AWS::EC2::NatGateway | EC2.40 |
| | AWS::EC2::NetworkAcl | EC2.16<br>EC2.21<br>EC2.41 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::EC2::NetworkInterface | EC2.22<br>EC2.35<br>EC2.180 |
| | AWS::EC2::PrefixList | EC2.176 |
| | AWS::EC2::RouteTable | EC2.42 |
| | AWS::EC2::SecurityGroup | EC2.2<br>EC2.13<br>EC2.14<br>EC2.18<br>EC2.19<br>EC2.43 |
| | AWS::EC2::SnapshotBlockPublicAccess | EC2.182 |
| | AWS::EC2::SpotFleet | EC2.173 |
| | AWS::EC2::Subnet | EC2.15<br>EC2.44<br>ElastiCache.7 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::EC2::TrafficMirrorFilter | EC2.178 |
| | AWS::EC2::TrafficMirrorSession | EC2.177 |
| | AWS::EC2::TrafficMirrorTarget | EC2.179 |
| | AWS::EC2::TransitGateway | EC2.23<br>EC2.52 |
| | AWS::EC2::TransitGatewayAttachment | EC2.33 |
| | AWS::EC2::TransitGatewayRouteTable | EC2.34 |
| | AWS::EC2::Volume | EC2.3<br>EC2.45 |
| | AWS::EC2::VPC | EC2.6<br>EC2.46 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::EC2::VPCBlockPublicAccessOptions` | EC2.172 |
| | `AWS::EC2::VPCEndpointService` | EC2.47 |
| | `AWS::EC2::VPCPeeringConnection` | EC2.49 |
| | `AWS::EC2::VPNConnection` | EC2.20<br>EC2.171<br>EC2.183 |
| | `AWS::EC2::VPNGateway` | EC2.50 |
| Amazon EC2 오토 스케일링 | `AWS::AutoScaling::AutoScalingGroup` | AutoScaling.1<br>AutoScaling.2<br>AutoScaling.6<br>AutoScaling.9<br>AutoScaling.10 |
| | `AWS::AutoScaling::LaunchConfiguration` | AutoScaling.3<br>Autoscaling.5 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| 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<br>ECR.3<br>ECR.5 |
| Amazon Elastic Container Service(Amazon ECS) | `AWS::ECS::Cluster` | ECS.12<br>ECS.14 |
| | `AWS::ECS::CapacityProvider` | ECS.19 |
| | `AWS::ECS::Service` | ECS.2<br>ECS.10<br>ECS.13 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::ECS::TaskDefinition` | ECS.3<br>ECS.4<br>ECS.5<br>ECS.8<br>ECS.9<br>ECS.15<br>ECS.17<br>ECS.18<br>ECS.20<br>ECS.21 |
| | `AWS::ECS::TaskSet` | ECS.16 |
| Amazon Elastic File System(Amazon EFS) | `AWS::EFS::AccessPoint` | EFS.3<br>EFS.4<br>EFS.5 |
| | `AWS::EFS::FileSystem` | EFS.7<br>EFS.8 |
| Amazon Elastic Kubernetes Service(Amazon EKS) | `AWS::EKS::Cluster` | EKS.2<br>EKS.6<br>EKS.8 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::EKS::Identity ProviderConfig` | EKS.7 |
| | `AWS::EKS::Nodegroup` | EKS.9 |
| AWS Elastic Beanstalk | `AWS::ElasticBeanstalk::Environment` | ElasticBeanstalk.1<br>ElasticBeanstalk.2<br>ElasticBeanstalk.3 |
| Elastic Load Balancing | `AWS::ElasticLoadBalancing::LoadBalancer` | ELB.2<br>ELB.3<br>ELB.5<br>ELB.7<br>ELB.8<br>ELB.9<br>ELB.10<br>ELB.14 |
| | `AWS::ElasticLoadBalancingV2::Listener` | ELB.17<br>ELB.18 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::ElasticLoadBalancingV2::LoadBalancer` | ELB.1<br>ELB.4<br>ELB.5<br>ELB.6<br>ELB.12<br>ELB.13<br>ELB.16 |
| ElasticSearch | `AWS::Elasticsearch::Domain` | ES.3<br>ES.4<br>ES.5<br>ES.6<br>ES.7<br>ES.8<br>ES.9 |
| Amazon EMR | `AWS::EMR::SecurityConfiguration` | EMR.3<br>EMR.4 |
| Amazon EventBridge | `AWS::Events::EventBus` | EventBridge.2<br>EventBridge.3 |
| | `AWS::Events::Endpoint` | EventBridge.4 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| 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<br>Glue.4 |
| | `AWS::Glue::MLTransform` | Glue.3 |
| Amazon GuardDuty | `AWS::GuardDuty::Detector` | GuardDuty.4 |
| | `AWS::GuardDuty::Filter` | GuardDuty.2 |
| | `AWS::GuardDuty::IPSet` | GuardDuty.3 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| AWS Identity and Access Managemen t(IAM) | `AWS::IAM::Group` | IAM.27<br>KMS.2 |
| | `AWS::IAM: :Policy` | IAM.1<br>IAM.21<br>KMS.1 |
| | `AWS::IAM::Role` | IAM.24<br>IAM.27<br>KMS.2 |
| | `AWS::IAM::User` | IAM.2<br>IAM.3<br>IAM.5<br>IAM.8<br>IAM.19<br>IAM.22<br>IAM.25<br>IAM.27<br>KMS.2 |
| AWS Identity and Access Management Access Analyzer | `AWS::Acce ssAnalyze r::Analyzer` | IAM.23 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| 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 이벤트 | `AWS::IoTEvents::AlarmModel` | IoTEvents.3 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `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 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `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 (Apache Cassandra 용) | `AWS::Cassandra::Keyspace` | Keyspaces.1 |
| Amazon Kinesis | `AWS::Kinesis::Stream` | Kinesis.1<br>Kinesis.2<br>Kinesis.3 |
| AWS Key Management Service(AWS KMS) | `AWS::KMS::Alias` | S3.17 |
| | `AWS::KMS::Key` | KMS.3<br>KMS.5<br>S3.17 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| AWS Lambda | `AWS::Lambda::Function` | Lambda.1<br>Lambda.2<br>Lambda.3<br>Lambda.5<br>Lambda.6<br>Lambda.7 |
| Amazon MSK | `AWS::MSK::Cluster` | MSK.1<br>MSK.2<br>MSK.4<br>MSK.6 |
| | `AWS::KafkaConnect::Connector` | MSK.3<br>MSK.5 |
| Amazon MQ | `AWS::AmazonMQ::Broker` | MQ.2<br>MQ.4<br>MQ.5<br>MQ.6 |
| AWS Network Firewall | `AWS::NetworkFirewall::Firewall` | NetworkFirewall.1<br>NetworkFirewall.7<br>NetworkFirewall.9<br>NetworkFirewall.10 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::NetworkFirewall::FirewallPolicy` | NetworkFirewall.3<br>NetworkFirewall.4<br>NetworkFirewall.5<br>NetworkFirewall.8 |
| | `AWS::NetworkFirewall::RuleGroup` | NetworkFirewall.6 |
| Amazon OpenSearch Service | `AWS::OpenSearch::Domain` | Opensearch.1<br>Opensearch.2<br>Opensearch.3<br>Opensearch.4<br>Opensearch.5<br>Opensearch.6<br>Opensearch.7<br>Opensearch.8<br>Opensearch.9<br>Opensearch.10<br>Opensearch.11 |
| AWS Private CA | `AWS::ACMPCA::CertificateAuthority` | PCA.2 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| Amazon Relational Database Service(Amazon RDS) | `AWS::RDS::DBCluster` | DocumentDB.1<br>DocumentDB.2<br>DocumentDB.4<br>DocumentDB.5<br>Neptune.1<br>Neptune.2<br>Neptune.4<br>Neptune.5<br>Neptune.7<br>Neptune.8<br>Neptune.9<br>RDS.7<br>RDS.12<br>RDS.14<br>RDS.15<br>RDS.16<br>RDS.24<br>RDS.27<br>RDS.28<br>RDS.34<br>RDS.35 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | | RDS.37<br>RDS.47<br>RDS.48 |
| | `AWS::RDS::DBClusterSnapshot` | DocumentDB.3<br>Neptune.3<br>Neptune.6<br>RDS.1<br>RDS.4<br>RDS.29 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::RDS::DBInstance | RDS.2<br>RDS.3<br>RDS.5<br>RDS.6<br>RDS.8<br>RDS.9<br>RDS.10<br>RDS.11<br>RDS.13<br>RDS.17<br>RDS.23<br>RDS.25<br>RDS.30<br>RDS.36<br>RDS.40 |
| | AWS::RDS::DBSecurityGroup | RDS.31 |
| | AWS::RDS::DBSnapshot | RDS.1<br>RDS.4<br>RDS.32 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::RDS::DBSubnetGroup | RDS.33 |
| | AWS::RDS::EventSubscription | RDS.19<br>RDS.20<br>RDS.21<br>RDS.22 |
| | AWS::RDS::GlobalCluster | RDS.51 |
| Amazon Redshift | AWS::Redshift::Cluster | Redshift.1<br>Redshift.2<br>Redshift.3<br>Redshift.4<br>Redshift.6<br>Redshift.7<br>Redshift.8<br>Redshift.10<br>Redshift.11<br>Redshift.18 |
| | AWS::Redshift::ClusterParameterGroup | Redshift.2<br>Redshift.17 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::Redshift::ClusterSnapshot` | Redshift.13 |
| | `AWS::Redshift::ClusterSubnetGroup` | Redshift.14<br>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<br>S3.3 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::S3::Bucket | CloudTrail.6<br>CloudTrail.7<br>S3.2<br>S3.3<br>S3.5<br>S3.6<br>S3.7<br>S3.8<br>S3.9<br>S3.10<br>S3.11<br>S3.12<br>S3.13<br>S3.14<br>S3.15<br>S3.17<br>S3.20 |
| | AWS::S3::MultiRegionAccessPoint | S3.24 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `AWS::S3Express::DirectoryBucket` | S3.25 |
| Amazon SageMaker AI | `AWS::SageMaker::AppImageConfig` | SageMaker.6 |
| | `AWS::SageMaker::Image` | SageMaker.7 |
| | `AWS::SageMaker::InferenceExperiment` | SageMaker.23<br>SageMaker.24 |
| | `AWS::SageMaker::Model` | SageMaker.5<br>SageMaker.16<br>SageMaker.19 |
| | `AWS::SageMaker::ModelExplainabilityJobDefinition` | SageMaker.20 |
| | `AWS::SageMaker::ModelQualityJobDefinition` | SageMaker.25 |
| | `AWS::SageMaker::MonitoringSchedule` | SageMaker.22 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | AWS::SageMaker::NotebookInstance | SageMaker.2<br>SageMaker.3<br>SageMaker.21 |
| | AWS::SageMaker::FeatureGroup | SageMaker.17<br>SageMaker.18 |
| AWS Secrets Manager | AWS::SecretsManager::Secret | SecretsManager.1<br>SecretsManager.2<br>SecretsManager.5 |
| AWS Service Catalog | AWS::ServiceCatalog::Portfolio | ServiceCatalog.1 |
| Amazon Simple Email Service(Amazon SES) | AWS::SES::ConfigurationSet | SES.2<br>SES.3 |
| | AWS::SES::ContactList | SES.1 |
| Amazon Simple Notification Service(Amazon SNS) | AWS::SNS::Topic | SNS.1<br>SNS.3<br>SNS.4 |
| Amazon Simple Queue Service(Amazon SQS) | AWS::SQS::Queue | SQS.1<br>SQS.2<br>SQS.3 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| 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<br>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<br>WAF.8 |

| AWS 서비스 | 조건 키 | 관련 제어 |
| --- | --- | --- |
| | `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<br>WAF.11 |
| Amazon WorkSpaces | `AWS::WorkSpaces::WorkSpace` | WorkSpaces.1<br>WorkSpaces.2 |

AWS기본 보안 모범 사례 표준에 필요한 리소스

Security Hub CSPM이 AWS기본 보안 모범 사례 표준(v.1.0.0)에 적용되고 활성화되며 AWS Config규칙을 사용하는 변경 트리거 제어에 대한 조사 결과를 정확하게 보고하려면 다음 유형의 리소스를에 기록해야 합니다AWS Config. 이 표준에 대한 자세한 내용은 AWS Security Hub CSPM의 기본 보안 모범 사례 표준 섹션을 참조하세요.

| AWS 서비스 | 조건 키 |
| --- | --- |
| Amazon API Gateway | `AWS::ApiGateway::DomainName` , `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| AWS AppSync | `AWS::AppSync::ApiCache` , `AWS::AppSync::GraphQLApi` |
| AWS Backup | `AWS::Backup::RecoveryPoint` |
| Amazon Bedrock | `AWS::Bedrock::DataSource` |
| Amazon Bedrock 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` |
| Amazon Connect Customer | `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` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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::Snapshot` `BlockPublicAccess` , `AWS::EC2::SpotFleet` , `AWS::EC2::Subnet` , `AWS::EC2::TransitGateway` , `AWS::EC2::VPCBlockPublicAccessOptions` , `AWS::EC2::VPNConnection` , `AWS::EC2::Volume` |
| Amazon EC2 오토 스케일링 | `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` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |
| Amazon OpenSearch Service | `AWS::OpenSearch::Domain` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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 Serverless | `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` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |

CIS AWS파운데이션 벤치마크에 필요한 리소스

인터넷 보안 센터(CIS) AWS기반 벤치마크에 적용되는 활성화된 제어에 대한 보안 검사를 실행하기 위해 Security Hub CSPM은 검사에 대해 규정된 정확한 감사 단계를 실행하거나 특정 AWS Config관리형 규칙을 사용합니다. Security Hub CSPM의 이 표준에 대한 자세한 내용은 Security Hub CSPM의 CIS AWS 파운데이션 벤치마크 섹션을 참조하세요.

CIS v5.0.0에 필요한 리소스

Security Hub CSPM이 AWS Config규칙을 사용하는 활성화된 CIS v5.0.0 변경 트리거 제어에 대한 결과를 정확하게 보고하려면에 다음 유형의 리소스를 기록해야 합니다AWS Config.

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |
| AWS Identity and Access Management(IAM) | `AWS::IAM::Group` , `AWS::IAM::User` , `AWS::IAM::Role` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| Amazon Relational Database Service(Amazon RDS) | `AWS::RDS::DBInstance` , `AWS::RDS::DBCluster` |
| Amazon Simple Storage Service(S3) | `AWS::S3::Bucket` |

CIS v3.0.0에 필요한 리소스

Security Hub CSPM이 AWS Config규칙을 사용하는 활성화된 CIS v3.0.0 변경 트리거 제어에 대한 결과를 정확하게 보고하려면에 다음 유형의 리소스를 기록해야 합니다AWS Config.

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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(S3) | `AWS::S3::Bucket` |

CIS v1.4.0에 필요한 리소스

Security Hub CSPM이 AWS Config규칙을 사용하는 활성화된 CIS v1.4.0 변경 트리거 제어에 대한 결과를 정확하게 보고하려면에 다음 유형의 리소스를 기록해야 합니다AWS Config.

| AWS 서비스 | 조건 키 |
| --- | --- |
| Amazon Elastic Compute Cloud(Amazon EC2) | `AWS::EC2::NetworkAcl` , `AWS::EC2::SecurityGroup` |
| AWS Identity and Access Management(IAM) | `AWS::IAM::Policy` , `AWS::IAM::User` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| Amazon Relational Database Service(Amazon RDS) | `AWS::RDS::DBInstance` |
| Amazon Simple Storage Service(S3) | `AWS::S3::Bucket` |

CIS v1.2.0에 필요한 리소스

Security Hub CSPM이 AWS Config규칙을 사용하는 활성화된 CIS v1.2.0 변경 트리거 제어에 대한 결과를 정확하게 보고하려면에 다음 유형의 리소스를 기록해야 합니다AWS Config.

| AWS 서비스 | 조건 키 |
| --- | --- |
| Amazon Elastic Compute Cloud(Amazon EC2) | `AWS::EC2::SecurityGroup` |
| AWS Identity and Access Management(IAM) | `AWS::IAM::Policy` , `AWS::IAM::User` |

NIST SP 800-53 개정 5 표준에 필요한 리소스

Security Hub CSPM이 NIST SP 800-53 개정 5 표준에 적용되고 활성화되며 AWS Config규칙을 사용하는 변경 트리거 제어에 대한 결과를 정확하게 보고하려면 다음 유형의 리소스를에 기록해야 합니다 AWS Config. 이 표준에 대한 자세한 내용은 Security Hub CSPM의 NIST SP 800-53 개정 5 섹션을 참조하세요.

| AWS 서비스 | 조건 키 |
| --- | --- |
| Amazon API Gateway | `AWS::ApiGateway::Stage` , `AWS::ApiGatewayV2::Stage` |
| AWS AppSync | `AWS::AppSync::GraphQLApi` |
| AWS Backup | `AWS::Backup::RecoveryPoint` |
| Amazon Bedrock AgentCore | `AWS::BedrockAgentCore::Gateway` , `AWS::BedrockAgentCore::Memory` |
| AWS Certificate Manager(ACM) | `AWS::ACM::Certificate` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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 오토 스케일링 | `AWS::AutoScaling::AutoScalingGroup` , `AWS::AutoScaling::LaunchConfiguration` |
| Amazon Elastic Container Registry(Amazon ECR) | `AWS::ECR::Repository` |
| Amazon Elastic Container Service(Amazon ECS) | `AWS::ECS::Cluster` , `AWS::ECS::Service` , `AWS::ECS::TaskDefinition` |
| Amazon Elastic File System(Amazon EFS) | `AWS::EFS::AccessPoint` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |
| Amazon MQ | `AWS::AmazonMQ::Broker` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| AWS Network Firewall | `AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup` |
| Amazon OpenSearch Service | `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(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` |
| AWS Secrets Manager | `AWS::SecretsManager::Secret` |
| AWS Transfer Family | `AWS::Transfer::Connector` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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 |

NIST SP 800-171 개정 2 표준에 필요한 리소스

Security Hub CSPM이 NIST SP 800-171 개정 2 표준에 적용되고 활성화되며 AWS Config규칙을 사용하는 변경 트리거 제어에 대한 결과를 정확하게 보고하려면 다음 유형의 리소스를에 기록해야 합니다AWS Config. 이 표준에 대한 자세한 내용은 Security Hub CSPM의 NIST SP 800-171 개정 2 섹션을 참조하세요.

| AWS 서비스 | 조건 키 |
| --- | --- |
| AWS Certificate Manager(ACM) | AWS::ACM::Certificate |
| Amazon API Gateway | AWS::ApiGateway::Stage |
| Amazon CloudFront | AWS::CloudFront::Distribution |
| Amazon CloudWatch | AWS::CloudWatch::Alarm |
| Amazon Elastic Compute Cloud(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 서비스 | 조건 키 |
| --- | --- |
| AWS Network Firewall | `AWS::NetworkFirewall::FirewallPolicy` , `AWS::NetworkFirewall::RuleGroup` |
| Amazon Simple Storage Service(Amazon S3) | `AWS::S3::Bucket` |
| Amazon Simple Notification Service(Amazon SNS) | `AWS::SNS::Topic` |
| AWS Systems Manager(SSM) | `AWS::SSM::PatchCompliance` |
| AWS WAF | `AWS::WAFv2::RuleGroup` |

PCI DSS v3.2.1에 필요한 리소스

Security Hub CSPM이 Payment Card Industry Data Security Standard(PCI DSS) v3.2.1에 적용되고 활성화되었으며 AWS Config 규칙을 사용하는 제어에 대한 조사 결과를 정확하게 보고하려면 다음 유형의 리소스를 AWS Config에 기록해야 합니다. 이 표준에 대한 자세한 내용은 Security Hub CSPM의 PCI DSS 섹션을 참조하세요.

| AWS 서비스 | 조건 키 |
| --- | --- |
| AWS CodeBuild | `AWS::CodeBuild::Project` |
| Amazon Elastic Compute Cloud(Amazon EC2) | `AWS::EC2::EIP` , `AWS::EC2::Instance` , `AWS::EC2::SecurityGroup` |
| Amazon EC2 오토 스케일링 | `AWS::AutoScaling::AutoScalingGroup` |
| AWS Identity and Access Management(IAM) | `AWS::IAM::Policy` , `AWS::IAM::User` |
| AWS Lambda | `AWS::Lambda::Function` |
| Amazon OpenSearch Service | `AWS::OpenSearch::Domain` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |

리소스 태그 지정 표준에 필요한 AWS리소스

AWS리소스 태그 지정 표준에 적용되는 모든 제어는 변경이 트리거되고 AWS Config규칙을 사용합니다. Security Hub CSPM이 이러한 제어에 대한 조사 결과를 정확하게 보고하려면 다음 유형의 리소스를에 기록해야 합니다AWS Config. 이 표준에 대한 자세한 내용은 AWS Security Hub CSPM의 리소스 태그 지정 표준 섹션을 참조하세요.

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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::ConfigurationProfile` , `AWS::AppConfig::Environment` , `AWS::AppConfig::ExtensionAssociation` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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 |
| Amazon Connect Customer | AWS::CustomerProfiles::ObjectType |
| AWS Database Migration Service(AWS DMS) | AWS::DMS::Certificate , AWS::DMS::EventSubscription<br><br>AWS::DMS::ReplicationInstance , AWS::DMS::ReplicationSubnetGroup |
| AWS DataSync | AWS::DataSync::Task |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |
| Amazon EC2 오토 스케일링 | `AWS::AutoScaling::AutoScalingGroup` |
| Amazon Elastic Container Registry(Amazon ECR) | `AWS::ECR::PublicRepository` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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`<br><br>`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` |
| AWS Identity and Access Management Access Analyzer(IAM Access Analyzer) | `AWS::AccessAnalyzer::Analyzer` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| AWS IoT | AWS::IoT::Authorizer , AWS::IoT::Dimension , AWS::IoT::MitigationAction , AWS::IoT::Policy , AWS::IoT::RoleAlias , AWS::IoT::SecurityProfile |
| AWS IoT이벤트 | 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 IoT무선 | 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(Apache Cassandra용) | AWS::Cassandra::Keyspace |
| Amazon Kinesis | AWS::Kinesis::Stream |
| AWS Lambda | AWS::Lambda::Function |
| Amazon MQ | AWS::AmazonMQ::Broker |

| AWS 서비스 | 조건 키 |
| --- | --- |
| AWS Network Firewall | `AWS::NetworkFirewall::Firewall` , `AWS::NetworkFirewall::FirewallPolicy` |
| Amazon OpenSearch Service | `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` |
| Amazon Simple Queue Service(Amazon SQS) | `AWS::SQS::Queue` |

| AWS 서비스 | 조건 키 |
| --- | --- |
| 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` |

## 보안 검사 실행 예약

보안 표준을 활성화하면 AWSSecurity Hub CSPM은 2시간 이내에 모든 검사를 실행하기 시작합니다. 대부분의 검사는 25분 이내에 실행되기 시작합니다. Security Hub CSPM은 제어의 기반이 되는 규칙을 평가하여 검사를 실행합니다. 제어가 첫 번째 검사 실행을 완료할 때까지 상태는 데이터 없음입니다.

새 표준을 활성화하면 Security Hub CSPM이 활성화된 다른 표준에서 활성화된 제어와 동일한 기본 AWS Config서비스 연결 규칙을 사용하는 제어에 대한 조사 결과를 생성하는 데 최대 24시간이 걸릴 수 있습니다. 예를 들어 AWS기본 보안 모범 사례(FSBP) 표준에서 Lambda.1 제어를 활성화하면 Security Hub CSPM은 서비스 연결 규칙을 생성하고 일반적으로 몇 분 내에 결과를 생성합니다. 이후 PCI DSS(지불 카드 산업 데이터 보안 표준)에서 Lambda.1 제어를 활성화하면, Security Hub CSPM은 동일한 서비스 연결 규칙을 사용하기 때문에 이 제어에 대한 조사 결과를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

초기 검사 후 각 제어에 대한 일정은 주기적이거나 변경으로 트리거될 수 있습니다. 관리형 AWS Config규칙을 기반으로 하는 제어의 경우 제어 설명에는 AWS Config개발자 안내서의 규칙 설명에 대한 링크가 포함됩니다. 이 설명은 규칙이 변경으로 트리거되는지 또는 주기적인지 여부를 표시합니다.

정기 보안 검사

정기적인 검사는 가장 최근 실행 후 12~24시간 이내에 자동으로 실행됩니다. Security Hub CSPM은 주기를 결정하며 사용자는 이를 변경할 수 없습니다. 주기적 제어에는 검사가 실행되는 시점의 평가가 반영됩니다.

주기적 제어 조사 결과의 워크플로 상태를 업데이트하고 다음 검사에서 조사 결과의 규정 준수 상태가 동일하게 유지되는 경우, 워크플로 상태는 수정된 상태로 유지됩니다. 예를 들어 KMS.4 컨트롤에 대해

실패한 결과가 있는 경우(AWS KMS key회전을 활성화해야 함) 결과를 수정하면 Security Hub CSPM은 워크플로 상태를에서 NEW로 변경합니다RESOLVED. 다음 정기 검사 전에 KMS 키 교체를 비활성화해도 검색 조사 결과의 워크플로 상태는 RESOLVED(으)로 유지됩니다.

Security Hub CSPM 사용자 지정 Lambda 함수를 사용하는 점검은 주기적입니다.

변경 트리거 보안 검사

변경 트리거 보안 검사는 연결된 리소스가 상태를 변경할 때 실행AWS Config됩니다. 리소스 상태의 변경 사항에 대한 지속적인 기록과 일일 기록 중에서 선택할 수 있습니다. 일일 기록을 선택하면 리소스 상태가 변경될 경우 각 24시간이 끝날 때마다 리소스 구성 데이터를 AWS Config전달합니다. 변경 사항이 없는 경우에는 데이터가 제공되지 않습니다. 이로 인해 24시간이 완료될 때까지 Security Hub CSPM 조사 결과 생성이 지연될 수 있습니다. 선택한 기록 기간에 관계없이 Security Hub CSPMAWS Config은 최소 24시간마다 한 번 확인하여의 리소스 업데이트가 누락되지 않았는지 확인합니다.

일반적으로 Security Hub CSPM은 가능한 경우, 항상 변경으로 트리거되는 규칙을 사용합니다. 리소스가 변경 트리거 규칙을 사용하려면 AWS Config구성 항목을 지원해야 합니다.

## 제어 조사 결과 생성 및 업데이트

AWSSecurity Hub CSPM은 보안 제어에 대한 검사를 실행할 때 제어 조사 결과를 생성하고 업데이트합니다. 제어 조사 결과는 AWS Security Finding Format(ASFF)을 사용합니다.

Security Hub CSPM은 일반적으로 제어에 대한 각 보안 검사에 대해 요금을 부과합니다. 그러나 여러 제어가 동일한 AWS Config규칙을 사용하는 경우 Security Hub CSPM은 규칙에 대해 각 검사에 대해 한 번만 요금을 부과합니다. 예를 들어 AWS Configiam-password-policy 규칙은 CISAWS 파운데이션 벤치마크 표준 및 AWS기본 보안 모범 사례 표준의 여러 제어에서 사용됩니다. Security Hub CSPM에서 해당 규칙에 대해 검사를 실행할 때마다 관련 제어 각각에 대해 별도의 제어 조사 결과가 생성되지만 검사 요금은 한 번만 청구됩니다.

제어 조사 결과의 크기가 최대 240KB를 초과하는 경우 Security Hub CSPM은 조사 결과에서 Resource.Details 객체를 제거합니다. 리소스가AWS Config 지원하는 제어의 경우 AWS Config콘솔을 사용하여 리소스 세부 정보를 검토할 수 있습니다.

주제

- 통합 제어 조사 결과
- 제어 조사 결과 생성, 업데이트 및 보관
- 제어 조사 결과 자동화 및 억제

- 제어 조사 결과에 대한 규정 준수 세부 정보
- 제어 조사 결과의 ProductFields 세부 정보
- 제어 조사 결과의 심각도 수준

통합 제어 조사 결과

계정에 통합 제어 조사 결과가 활성화되어 있는 경우 Security Hub CSPM은 제어가 활성화된 여러 표준에 적용되는 경우에도 제어의 각 보안 검사에 대해 하나의 새로운 조사 결과 또는 조사 결과 업데이트를 생성합니다. 제어 및 해당 제어가 적용되는 표준의 목록을 보려면 Security Hub CSPM 제어 참조 섹션을 참조하세요. 조사 결과 노이즈를 줄이려면 통합 제어 조사 결과를 활성화하는 것이 좋습니다.

2023년 2월 23일 AWS 계정이전에에 대해 Security Hub CSPM을 활성화한 경우이 섹션 뒷부분의 지침에 따라 통합 제어 조사 결과를 활성화할 수 있습니다. 2023년 2월 23일 또는 그 이후에 Security Hub CSPM을 활성화하면 계정에서 통합 제어 조사 결과가 자동으로 활성화됩니다.

Security Hub CSPM과 AWS Organizations 통합을 사용하거나 수동 초대 프로세스를 통해 초대된 멤버 계정을 사용할 때는 관리자 계정에서 활성화된 경우에만 멤버 계정에서 통합 제어 조사 결과가 활성화됩니다. 관리자 계정에서 이 기능을 비활성화하면 멤버 계정에서도 해당 기능이 비활성화됩니다. 이 동작은 새로운 및 기존 구성원 계정에 적용됩니다. 또한 관리자가 중앙 구성을 사용하여 여러 계정에 대한 Security Hub CSPM을 관리하는 경우 중앙 구성 정책을 사용하여 계정의 통합 제어 조사 결과를 활성화하거나 비활성화할 수 없습니다.

계정에서 통합 제어 조사 결과를 비활성화하면 Security Hub CSPM은 제어를 포함하는 활성화된 표준 각각에 대해 별도의 제어 조사 결과를 생성하거나 업데이트합니다. 예를 들어, 제어를 공유하는 4개의 표준을 활성화하면 해당 제어에 대한 보안 검사 후 4개의 개별 조사 결과를 받게 됩니다. 통합 제어 조사 결과를 활성화하면 조사 결과가 하나만 수신됩니다.

통합 제어 조사 결과를 활성화하면 Security Hub CSPM은 표준에 구애받지 않는 새로운 조사 결과를 생성하고 원래 표준 기반 조사 결과를 보관합니다. 일부 제어 조사 결과 필드 및 값이 변경되어 기존 워크플로에 영향을 미칠 수 있습니다. 이러한 변경에 대한 자세한 내용은 통합 제어 조사 결과 - ASFF 변경 섹션을 참조하세요. 통합 제어 조사 결과를 활성화하면 통합된 서드 파티 제품이 Security Hub CSPM에서 수신하는 조사 결과에도 영향을 미칠 수 있습니다. AWSv2.0.0에서 자동 보안 대응 솔루션을 사용하는 경우 통합 제어 조사 결과를 지원한다는 점에 유의하세요.

통합 제어 조사 결과를 활성화하거나 비활성화하려면 관리자 계정 또는 독립형 계정으로 로그인해야 합니다.

> **Note**
>
> 통합 제어 조사 결과를 활성화한 후 Security Hub CSPM이 새로운 통합 조사 결과를 생성하고 기존 표준 기반 조사 결과를 보관하는 데 최대 24시간이 걸릴 수 있습니다. 통합 제어 조사 결과를 비활성화한 후 Security Hub CSPM에서 새로운 표준 기반 조사 결과를 생성하고 통합 조사 결과를 보관하는 데 최대 24시간이 걸릴 수 있습니다. 이 기간 동안 계정에서 표준에 구애받지 않는 조사 결과와 표준 기반 조사 결과가 혼합되어 표시될 수 있습니다.

Security Hub CSPM console

통합 제어 조사 결과를 활성화 또는 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 제어 섹션에서 편집을 선택합니다.
4. 통합 제어 조사 결과 스위치를 사용하여 통합 제어 조사 결과를 활성화하거나 비활성화합니다.
5. 저장을 선택합니다.

Security Hub CSPM API

통합 제어 조사 결과를 프로그래밍 방식으로 활성화하거나 비활성화하려면 Security Hub CSPM API의 UpdateSecurityHubConfiguration 작업을 사용합니다. 또는를 사용하는 경우 update-security-hub-configuration 명령을 AWS CLI실행합니다.

`control-finding-generator` 파라미터의 경우 `SECURITY_CONTROL`을 지정하여 통합 제어 조사 결과를 활성화합니다. 통합 제어 조사 결과를 비활성화하려면 `STANDARD_CONTROL`을 지정합니다.

예를 들어 다음 AWS CLI명령은 통합 제어 조사 결과를 활성화합니다.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

다음 AWS CLI명령은 통합 제어 조사 결과를 비활성화합니다.

```
$ aws securityhub  --region us-east-1 update-security-hub-configuration --control-finding-generator STANDARD_CONTROL
```

### 제어 조사 결과 생성, 업데이트 및 보관

Security Hub CSPM은 일정 따라 보안 검사를 실행합니다. Security Hub CSPM은 제어에 대한 보안 검사를 처음 실행할 때 제어가 확인하는 각 AWS리소스에 대해 새 결과를 생성합니다. Security Hub CSPM은 이후 제어에 대한 보안 검사를 실행할 때마다 기존 조사 결과를 업데이트하여 검사 결과를 보고합니다. 즉, 개별 조사 결과에서 제공하는 데이터를 사용하여 특정 리소스의 특정 제어에 대한 규정 준수 변경을 추적할 수 있습니다.

예를 들어, 특정 제어에서 리소스의 규정 준수 상태가 `FAILED`에서 `PASSED`로 변경되면 Security Hub CSPM은 새 조사 결과를 생성하지 않습니다. 대신, Security Hub CSPM은 제어 및 리소스에 대한 기존 조사 결과를 업데이트합니다. 조사 결과에서 Security Hub CSPM은 규정 준수 상태(`Compliance.Status`) 필드의 값을 `PASSED`로 변경합니다. 또한 Security Hub CSPM은 심각도 레이블, 워크플로 상태, Security Hub CSPM이 가장 최근에 검사를 실행하고 결과를 업데이트한 시점을 나타내는 타임스탬프와 같은 검사 결과를 반영하도록 추가 필드의 값을 업데이트합니다.

규정 준수 상태의 변경을 보고할 때 Security Hub CSPM은 제어 조사 결과에서 다음 필드를 업데이트할 수 있습니다.

- `Compliance.Status` – 리소스의 지정된 제어에 대한 새 규정 준수 상태입니다.
- `FindingProviderFields.Severity.Label` - 조사 결과의 심각도에 대한 새로운 정성적 표현입니다(예: `LOW`, `MEDIUM` 또는 `HIGH`).
- `FindingProviderFields.Severity.Original` - 조사 결과의 심각도에 대한 새로운 정량적 표현입니다(예: 규정 준수 리소스의 `0`).
- `FirstObservedAt` - 리소스의 규정 준수 상태가 가장 최근에 변경된 시점입니다.
- `LastObservedAt` - Security Hub CSPM이 가장 최근에 지정된 제어 및 리소스에 대한 보안 검사를 실행한 시점입니다.
- `ProcessedAt` - Security Hub CSPM이 가장 최근에 조사 결과를 처리하기 시작한 시점입니다.
- `ProductFields.PreviousComplianceStatus` – 리소스의 지정된 제어에 대한 이전 규정 준수 상태(`Compliance.Status`)입니다.
- `UpdatedAt` - Security Hub CSPM이 가장 최근에 조사 결과를 업데이트한 시점입니다.
- `Workflow.Status` - 리소스의 지정된 제어에 대한 새 규정 준수 상태를 기반으로 한 조사 결과에 대한 조사 상태입니다.

Security Hub CSPM이 필드를 업데이트하는지 여부는 주로 해당 제어 및 리소스에 대한 최신 보안 검사 결과에 따라 달라집니다. 예를 들어, 특정 제어에서 리소스의 규정 준수 상태가 `PASSED`에서 `FAILED`로 변경되면 Security Hub CSPM은 조사 결과의 워크플로 상태를 `NEW`로 변경합니다. 개별 조

사 결과에 대한 업데이트를 추적하려면 조사 결과 기록을 참조할 수 있습니다. 조사 결과의 개별 필드에 대한 자세한 내용은 AWS Security Finding Format(ASFF)을 참조하세요.

경우에 따라 Security Hub CSPM은 기존 조사 결과를 업데이트하는 대신 제어의 후속 검사에 대해 새 조사 결과를 생성합니다. 이는 제어를 지원하는 AWS Config규칙에 문제가 있는 경우 발생할 수 있습니다. 그러면 Security Hub CSPM은 기존 조사 결과를 보관하고 각 검사에 대해 새 조사 결과를 생성합니다. 새 조사 결과에서 규정 준수 상태는 `NOT_AVAILABLE`이고 레코드 상태는 `ARCHIVED`입니다. AWS Config규칙 문제를 해결한 후 Security Hub CSPM은 새 결과를 생성하고 업데이트를 시작하여 개별 리소스의 규정 준수 상태에 대한 후속 변경 사항을 추적합니다.

Security Hub CSPM은 제어 조사 결과를 생성하고 업데이트하는 것 외에도 특정 기준을 충족하는 제어 조사 결과를 자동으로 보관합니다. Security Hub CSPM은 제어가 비활성화되거나, 지정된 리소스가 삭제되거나, 지정된 리소스가 더 이상 존재하지 않는 경우 조사 결과를 보관합니다. 연결된 서비스가 현재 사용되지 않기 때문에 리소스가 더 이상 존재하지 않을 수 있습니다. 구체적으로, Security Hub CSPM은 조사 결과가 다음 기준 중 하나를 충족하는 경우 제어 조사 결과를 자동으로 보관합니다.

- 조사 결과가 3~5일 동안 업데이트되지 않은 경우. 이 기간을 기반으로 한 보관은 BEB(best-effort basis) 방식이며 보장되지 않습니다.
- 지정된 리소스의 규정 준수 상태에 `NOT_APPLICABLE` 대해 반환된 관련 AWS Config평가입니다.

조사 결과가 보관되었는지 확인하려면 조사 결과의 레코드 상태(`RecordState`) 필드를 참조할 수 있습니다. 조사 결과가 보관된 경우 이 필드의 값은 `ARCHIVED`입니다.

Security Hub CSPM은 보관된 제어 조사 결과를 30일 동안 저장합니다. 30일이 경과하면 조사 결과가 만료되고 Security Hub CSPM이 조사 결과를 영구적으로 삭제합니다. 보관된 제어 조사 결과가 만료되었는지 확인하기 위해 Security Hub CSPM은 조사 결과의 `UpdatedAt` 필드 값을 기반으로 계산합니다.

보관된 제어 조사 결과를 30일 이상 저장하려면 조사 결과를 S3 버킷으로 내보낼 수 있습니다. 이 작업은 Amazon EventBridge 규칙과 함께 사용자 지정 작업을 사용하여 수행할 수 있습니다. 자세한 내용은 자동 응답 및 문제 해결을 위해 EventBridge 사용 단원을 참조하십시오.

> **Note**
>
> 2025년 7월 3일 이전에 Security Hub CSPM은 리소스의 제어 규정 준수 상태가 변경될 때 제어 조사 결과를 다르게 생성하고 업데이트했습니다. 이전에는 Security Hub CSPM이 리소스에 대해 새 제어 조사 결과를 생성하고 기존 조사 결과를 보관했습니다. 따라서 조사 결과가 만료될 때까지(30일 후) 특정 제어 및 리소스에 대해 보관된 조사 결과가 여러 개 있을 수 있습니다.

### 제어 조사 결과 자동화 및 억제

Security Hub CSPM 자동화 규칙을 사용하여 특정 제어 조사 결과를 업데이트하거나 억제할 수 있습니다. 조사 결과를 억제하는 경우에도 해당 조사 결과에 계속 액세스할 수 있습니다. 그러나 억제는 조사 결과를 해결하는 데 조치가 필요하지 않다는 확신을 나타냅니다.

조사 결과를 억제하면 조사 결과 노이즈를 줄일 수 있습니다. 예를 들어 테스트 계정에서 생성된 제어 조사 결과를 억제할 수 있습니다. 또는 특정 리소스와 관련된 조사 결과를 억제할 수 있습니다. 조사 결과를 자동으로 업데이트하거나 억제하는 방법에 대한 자세한 내용은 Security Hub CSPM의 자동화 규칙 이해 섹션을 참조하세요.

자동화 규칙은 특정 제어 조사 결과를 업데이트하거나 억제하려는 경우에 적합합니다. 그러나 조직 또는 사용 사례와 관련이 없는 제어가 있는 경우 제어를 비활성화하는 것이 좋습니다. 제어를 비활성화하면 Security Hub CSPM이 해당 제어에 대한 보안 검사를 실행하지 않으며 요금이 부과되지 않습니다.

### 제어 조사 결과에 대한 규정 준수 세부 정보

제어에 대한 보안 검사에서 생성된 조사 결과에서 AWSSecurity Finding Format(ASFF)의 규정 준수 객체 및 필드는 제어가 확인한 개별 리소스에 대한 규정 준수 세부 정보를 제공합니다. 여기에는 다음 정보가 포함되어 있습니다.

- `AssociatedStandards` - 제어가 활성화되는 활성화된 표준입니다.
- `RelatedRequirements` - 사용 가능한 모든 표준의 제어 관련 요구 사항의 목록입니다. 이러한 요구 사항은 PCI DSS(지불 카드 산업 데이터 보안 표준) 또는 NIST SP 800-171 개정 2와 같은 제어를 위한 서드 파티 보안 프레임워크에서 나온 것입니다.
- `SecurityControlId` - Security Hub CSPM이 지원하는 보안 표준 전반의 제어를 위한 식별자입니다.
- `Status` - 특정 제어에 대해 Security Hub CSPM이 가장 최근에 실행한 검사의 결과입니다. 이전 검사 결과는 조사 결과 기록에 유지됩니다.
- `StatusReasons` - `Status` 필드에 지정된 값의 사유를 나열하는 배열입니다. 각 사유에는 사유 코드 및 설명이 포함됩니다.

다음 표에는 조사 결과가 `StatusReasons` 배열에 포함할 수 있는 사유 코드 및 설명이 나열되어 있습니다. 문제 해결 단계는 지정된 사유 코드로 조사 결과를 생성한 제어에 따라 달라집니다. 제어에 대한 문제 해결 지침을 검토하려면 Security Hub CSPM 제어 참조 섹션을 참조하세요.

| 사유 코드 | 규정 준수 상태 | 설명 |
| --- | --- | --- |
| CLOUDTRAIL_METRIC_FILTER_NOT_VALID | FAILED | 다중 리전 CloudTrail 추적에 유효한 메트릭 필터가 없습니다. |
| CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT | FAILED | 다중 리전 CloudTrail 추적에 메트릭 필터가 없습니다. |
| CLOUDTRAIL_MULTI_REGION_NOT_PRESENT | FAILED | 필요한 구성의 다중 리전 CloudTrail 추적이 계정에 없습니다. |
| CLOUDTRAIL_REGION_INVAILD | WARNING | 다중 리전 CloudTrail 추적이 현재 리전에 없습니다. |
| CLOUDWATCH_ALARM_ACTIONS_NOT_VALID | FAILED | 유효한 경보 작업이 없습니다. |
| CLOUDWATCH_ALARMS_NOT_PRESENT | FAILED | CloudWatch 경보가 계정에 존재하지 않습니다. |
| CONFIG_ACCESS_DENIED | NOT_AVAILABLE<br><br>AWS Config상태는 입니다. ConfigError | AWS Config액세스가 거부되었습니다.<br><br>AWS Config이 활성화되어 있고 충분한 권한이 부여되었는지 확인합니다. |
| CONFIG_EVALUATIONS_EMPTY | PASSED | AWS Config는 규칙을 기반으로 리소스를 평가했습니다.<br><br>규칙이 해당 범위의 AWS리소스에 적용되지 않았거나, 지정된 리소스가 삭제되었거나, 평가 결과가 삭제되었습니다. |
| CONFIG_RECORDER_CUSTOM_ROLE | FAILED(Config.1의 경우) | AWS Config레코더는 AWS Config 서비스 연결 역할 대신 사용자 지정 IAM 역할을 사용하며 Config.1의 includeConfigServi |

| 사유 코드 | 규정 준수 상태 | 설명 |
| --- | --- | --- |
| | | ceLinkedRoleCheck 사용자 지정 파라미터는 로 설정되지 않습니다false. |
| CONFIG_RECORDER_DISABLED | FAILED(Config.1의 경우) | AWS Config구성 레코더가 켜져 있으면가 활성화되지 않습니다. |
| CONFIG_RECORDER_MISSING_REQUIRED_RESOURCE_TYPES | FAILED(Config.1의 경우) | AWS Config는 활성화된 Security Hub CSPM 제어에 해당하는 모든 리소스 유형을 기록하지 않습니다. 다음 리소스에 대한 기록을 켜세요. ###### ###. |
| CONFIG_RETURNS_NOT_APPLICABLE | NOT_AVAILABLE | 가 해당 없음 상태를 AWS Config반환NOT_AVAILABLE 했기 때문에 규정 준수 상태는 입니다.<br><br>AWS Config는 상태의 이유를 제공하지 않습니다. 해당 없음 상태가 될 수 있는 몇 가지 이유는 다음과 같습니다.<br><br>• AWS Config규칙 범위에서 리소스가 제거되었습니다.<br>• AWS Config규칙이 삭제되었습니다.<br>• 리소스가 삭제되었습니다.<br>• AWS Config규칙 로직은 해당 없음 상태를 생성할 수 있습니다. |

| 사유 코드 | 규정 준수 상태 | 설명 |
| --- | --- | --- |
| CONFIG_RULE_EVALUATION_ERROR | NOT_AVAILABLE<br><br>AWS Config상태는 입니다. ConfigError | 이 사유 코드는 여러 가지 유형의 평가 오류에 사용됩니다.<br><br>설명에 구체적인 사유 정보가 나와 있습니다.<br><br>오류 유형은 다음 중 하나일 수 있습니다.<br><br>• 권한 부족으로 인해 평가를 수행할 수 없습니다. 설명에 누락된 특정 권한이 나와 있습니다.<br>• 파라미터의 값이 누락되었거나 잘못되었습니다. 설명에 파라미터 및 파라미터 값 요구 사항이 나와 있습니다.<br>• S3 버킷에서 읽는 중 오류가 발생했습니다. 설명에 해당 버킷이 식별되어 있고 구체적인 오류가 나와 있습니다.<br>• 누락된 AWS구독.<br>• 평가에 대한 전체 시간이 초과되었습니다.<br>• 일시 중지된 계정입니다. |
| CONFIG_RULE_NOT_FOUND | NOT_AVAILABLE<br><br>AWS Config상태는 입니다. ConfigError | AWS Config규칙이 생성 중입니다. |
| INTERNAL_SERVICE_ERROR | NOT_AVAILABLE | 알 수 없는 오류가 발생했습니다. |

| 사유 코드 | 규정 준수 상태 | 설명 |
| --- | --- | --- |
| LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE | FAILED | Security Hub CSPM은 사용자 지정 Lambda 런타임에 대해 검사를 수행할 수 없습니다. |
| S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION | WARNING | 이 규칙과 연결된 S3 버킷이 다른 리전 또는 계정에 있기 때문에 조사 결과가 WARNING 상태입니다.<br><br>이 규칙은 교차 리전 또는 교차 계정 확인을 지원하지 않습니다.<br><br>이 리전 또는 계정에서 이 제어를 비활성화하는 것이 좋습니다. 리소스가 있는 리전 또는 계정에서만 실행하세요. |
| SNS_SUBSCRIPTION_NOT_PRESENT | FAILED | CloudWatch Logs 메트릭 필터에 유효한 Amazon SNS 구독이 없습니다. |
| SNS_TOPIC_CROSS_ACCOUNT | WARNING | 검색 조사 결과가 WARNING 상태에 있습니다.<br><br>이 규칙과 관련된 SNS 주제는 다른 계정에서 소유하고 있습니다. 현재 계정으로는 구독 정보를 얻을 수 없습니다.<br><br>SNS 주제를 소유한 계정은 현재 계정에 해당 SNS 주제에 대한 sns:ListSubscriptionsByTopic 권한을 부여해야 합니다. |

| 사유 코드 | 규정 준수 상태 | 설명 |
| --- | --- | --- |
| SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION | WARNING | 이 규칙과 연결된 SNS 주제가 다른 리전 또는 계정에 있기 때문에 조사 결과가 WARNING 상태입니다.<br><br>이 규칙은 교차 리전 또는 교차 계정 확인을 지원하지 않습니다.<br><br>이 리전 또는 계정에서 이 제어를 비활성화하는 것이 좋습니다. 리소스가 있는 리전 또는 계정에서만 실행하세요. |
| SNS_TOPIC_INVALID | FAILED | 이 규칙과 관련된 SNS 주제는 유효하지 않습니다. |
| THROTTLING_ERROR | NOT_AVAILABLE | 관련 API 작업이 허용된 속도를 초과했습니다. |

제어 조사 결과의 ProductFields 세부 정보

제어에 대한 보안 검사에서 생성된 조사 결과에서 AWSSecurity Finding Format(ASFF)의 ProductFields 속성에는 다음 필드가 포함될 수 있습니다.

`ArchivalReasons:0/Description`

Security Hub CSPM이 조사 결과를 보관하는 이유를 설명합니다.

예를 들어, 제어 또는 표준을 비활성화하거나 통합 제어 조사 결과를 활성화/비활성화하면 Security Hub CSPM은 기존 조사 결과를 보관합니다.

`ArchivalReasons:0/ReasonCode`

Security Hub CSPM이 조사 결과를 보관한 이유를 표시합니다.

예를 들어, 제어 또는 표준을 비활성화하거나 통합 제어 조사 결과를 활성화/비활성화하면 Security Hub CSPM은 기존 조사 결과를 보관합니다.

`PreviousComplianceStatus`

조사 결과에 대한 가장 최근의 업데이트를 기준으로, 리소스의 지정된 제어에 대한 이전 규정 준수 상태(`Compliance.Status`)입니다. 가장 최근의 업데이트 중에 리소스의 규정 준수 상태가 변경

되지 않은 경우 이 값은 조사 결과의 Compliance.Status 필드의 값과 동일합니다. 가능한 값 목록은 규정 준수 상태 및 제어 상태 평가 단원을 참조하세요.

StandardsGuideArn 또는 StandardsArn

제어와 관련된 표준의 ARN입니다.

CIS AWS파운데이션 벤치마크 표준의 경우 필드는 입니다StandardsGuideArn. PCI DSS 및 AWS기본 보안 모범 사례 표준의 경우 필드는 입니다StandardsArn.

통합 제어 조사 결과를 활성화하면 이러한 필드는 Compliance.AssociatedStandards에 맞게 제거됩니다.

StandardsGuideSubscriptionArn 또는 StandardsSubscriptionArn

표준에 대한 계정 구독의 ARN입니다.

CIS AWS파운데이션 벤치마크 표준의 경우 필드는 입니다StandardsGuideSubscriptionArn. PCI DSS 및 AWS기본 보안 모범 사례 표준의 경우 필드는 입니다StandardsSubscriptionArn.

통합 제어 조사 결과를 활성화하면 이러한 필드는 제거됩니다.

RuleId 또는 ControlId

제어의 식별자입니다.

CIS AWS파운데이션 벤치마크 표준 버전 1.2.0의 경우 필드는 입니다RuleId. CIS AWS Foundations Benchmark 표준의 후속 버전을 포함한 다른 표준의 경우 필드는 ControlId입니다.

통합 제어 조사 결과를 활성화하면 이러한 필드는 Compliance.SecurityControlId에 맞게 제거됩니다.

RecommendationUrl

제어에 대한 문제 해결 정보의 URL입니다. 통합 제어 조사 결과를 켜면 이러한 필드는 Remediation.Recommendation.Url에 맞게 제거됩니다.

RelatedAWSResources:0/name

조사 결과와 연결된 리소스의 이름입니다.

RelatedAWSResource:0/type

제어에 연결된 리소스 유형입니다.

`StandardsControlArn`

제어의 ARN입니다. 통합 제어 조사 결과를 활성화하면 이러한 필드는 제거됩니다.

`aws/securityhub/ProductName`

제어 조사 결과의 경우, 제품 이름은 `Security Hub`입니다.

`aws/securityhub/CompanyName`

제어 조사 결과의 경우, 회사 이름은 `AWS`입니다.

`aws/securityhub/annotation`

제어를 통해 발견된 문제에 대한 설명입니다.

`aws/securityhub/FindingId`

조사 결과의 식별자입니다.

통합 제어 조사 결과를 활성화하면 이 필드는 표준을 참조하지 않습니다.

### 제어 조사 결과의 심각도 수준

Security Hub CSPM 제어에 할당된 심각도는 해당 제어의 중요성을 나타냅니다. 제어의 심각도에 따라 제어 조사 결과에 할당되는 심각도 레이블이 결정됩니다.

#### 심각도 기준

제어의 심각도는 다음 기준에 대한 평가를 기반으로 결정됩니다.

- 위협 행위자가 제어와 관련된 구성 약점을 악용하는 것은 얼마나 어려운가요? 난이도는 취약점을 이용해 위협 시나리오를 수행하는 데 필요한 정교함이나 복잡성의 정도에 따라 결정됩니다.
- 약점으로 인해 AWS 계정또는 리소스가 손상될 가능성은 얼마나 됩니까? AWS 계정또는 리소스가 손상되면 데이터 또는 AWS인프라의 기밀성, 무결성 또는 가용성이 어떤 식으로든 손상됩니다. 손상 가능성은 위협 시나리오로 인해 AWS 서비스또는 리소스가 중단되거나 침해될 가능성을 나타냅니다.

예를 들어, 다음 구성 약점을 고려해 보세요.

- 사용자 액세스 키는 90일마다 교체되지 않습니다.
- IAM 루트 사용자 키가 존재합니다.

두 약점 모두 공격자가 악용하기 어렵습니다. 두 경우 모두 공격자는 보안 인증 도용이나 다른 방법을 사용하여 사용자 키를 획득할 수 있습니다. 그런 다음 이를 사용하여 무단으로 리소스에 액세스할 수 있습니다.

하지만 위협 행위자가 루트 사용자 액세스 키를 획득하면 액세스 권한이 더 커지므로 보안 침해 가능성이 훨씬 높아집니다. 따라서 루트 사용자 키 취약점의 심각도가 더 높습니다.

심각도는 기본 리소스의 중요도를 고려하지 않습니다. 중요도는 조사 결과와 관련된 리소스의 중요도 수준입니다. 예를 들어, 미션 크리티컬 애플리케이션과 관련된 리소스와 비프로덕션 테스트와 관련된 리소스보다 더 중요합니다. 리소스 중요도 정보를 캡처하려면 AWSSecurity Finding Format(ASFF)의 `Criticality` 필드를 사용합니다.

다음 표에는 보안 레이블에 대한 악용 난이도과 손상 가능성이 나와 있습니다.

| | 침해 가능성이 매우 높음 | 침해 가능성이 있음 | 침해 가능성이 낮음 | 침해 가능성이 매우 낮음 |
|---|---|---|---|---|
| 악용하기 매우 쉬움 | 심각 | 심각 | 높음 | 중간 |
| 악용하기 다소 쉬움 | 심각 | 높음 | 중간 | 중간 |
| 악용하기가 다소 어려움 | 높음 | 중간 | 중간 | 낮음 |
| 악용하기가 매우 어려움 | 중간 | 중간 | 낮음 | 낮음 |

심각도 정의

심각도 레이블은 다음과 같이 정의됩니다.

심각 – 문제가 확대되는 것을 방지하려면 문제를 즉시 해결해야 합니다.

> 예를 들어, 개방형 S3 버킷은 심각한 조사 결과로 간주됩니다. 개방형 S3 버킷은 수많은 위협 행위자가 검색하기 때문에 노출된 S3 버킷의 데이터를 다른 사용자가 검색하고 액세스할 가능성이 있습니다.

일반적으로 공개적으로 액세스할 수 있는 리소스는 중요한 보안 문제로 간주됩니다. 중요한 발견은 최대한 긴급하게 처리해야 합니다. 리소스의 중요도도 고려해야 합니다.

높음 – 우선적으로 해결해야 할 문제입니다.

예를 들어, 기본 VPC 보안 그룹이 인바운드 및 아웃바운드 트래픽에 개방되어 있는 경우, 심각도가 높은 것으로 간주됩니다. 위협 행위자가 이 방법을 사용하면 VPC를 손상시키기가 다소 쉽습니다. 또한 위협 행위자가 VPC에 침투한 후에는 리소스를 방해하거나 외부로 유출할 수 있습니다.

Security Hub CSPM에서는 심각도가 높은 조사 결과를 단기 우선순위로 처리할 것을 권장합니다. 즉각적인 개선 조치를 취해야 합니다. 리소스의 중요도도 고려해야 합니다.

중간 - 이 문제는 중기 우선 순위로 다루어야 합니다.

예를 들어, 전송 중인 데이터에 대한 암호화가 이루어지지 않으면 심각도가 보통인 것으로 간주됩니다. 이 약점을 이용하려면 정교한 중간자 공격이 필요합니다. 바꿔 말하면 다소 어렵습니다. 위협 시나리오가 성공하면 일부 데이터가 손상될 수 있습니다.

Security Hub CSPM에서는 최대한 빨리 관련 리소스를 조사할 것을 권장합니다. 리소스의 중요도도 고려해야 합니다.

낮음 - 자체적으로 조치가 필요하지 않은 문제입니다.

예를 들어, 포렌식 정보를 수집하지 못하면 심각도가 낮은 것으로 간주됩니다. 이러한 제어는 향후 손상을 방지하는 데 도움이 될 수 있지만 포렌식이 없다고 해서 손상으로 직접 이어지지는 않습니다.

심각도가 낮은 조사 결과에 대해 즉각적인 조치를 취할 필요는 없지만, 다른 문제와 연관시킬 때 컨텍스트를 제공할 수 있습니다.

정보 - 구성 약점은 발견되지 않았습니다.

즉, `PASSED`, `WARNING` 또는 `NOT AVAILABLE` 상태입니다.

권장되는 조치는 없습니다. 정보 조사 결과는 고객이 규정 준수 상태에 있음을 입증하는 데 도움이 됩니다.

## 규정 준수 상태 및 제어 상태 평가

AWSSecurity Finding 형식의 `Compliance.Status` 필드는 제어 조사 결과의 결과를 설명합니다.AWSSecurity Hub CSPM은 제어 조사 결과의 규정 준수 상태를 사용하여 전체 제어 상태를 결정합니다. 제어 상태는 Security Hub CSPM 콘솔의 제어 세부 정보 페이지에 표시됩니다.

Security Hub CSPM 조사 결과의 규정 준수 상태 평가

각 결과의 규정 준수 상태는 다음 값 중 하나가 할당됩니다.

- PASSED - 제어가 조사 결과에 대한 보안 검사를 통과했음을 나타냅니다. 그러면 자동으로 Security Hub CSPM Workflow.Status가 RESOLVED로 설정됩니다.
- FAILED - 제어가 조사 결과에 대한 보안 검사를 통과하지 못했음을 나타냅니다.
- WARNING - Security Hub CSPM이 리소스가 PASSED 또는 FAILED 상태인지 확인할 수 없음을 나타냅니다. 예를 들어 해당 리소스 유형에 대해 AWS Config 리소스 기록이 켜져 있지 않습니다.
- NOT_AVAILABLE - 서버가 실패했거나, 리소스가 삭제되었거나, AWS Config평가 결과가 였기 때문에 검사를 완료할 수 없음을 나타냅니다NOT_APPLICABLE. AWS Config평가 결과가 인 경우 NOT_APPLICABLESecurity Hub CSPM은 자동으로 결과를 보관합니다.

조사 결과의 규정 준수 상태가 PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE로 변경되고 Workflow.Status가 NOTIFIED 또는 RESOLVED인 경우, Security Hub CSPM은 자동으로 Workflow.Status를 NEW로 변경합니다.

제어에 해당하는 리소스가 없는 경우, Security Hub CSPM은 계정 수준에서 PASSED 조사 결과를 생성합니다. 제어에 해당하는 리소스가 있지만 리소스를 삭제한 경우, Security Hub CSPM은 NOT_AVAILABLE 조사 결과를 생성하고 즉시 보관합니다. 18시간 후에는 제어에 해당하는 리소스가 더 이상 없기 때문에 PASSED 조사 결과를 수신하게 됩니다.

규정 준수 상태에서 제어 상태 도출

Security Hub CSPM은 제어 조사 결과의 규정 준수 상태를 사용하여 전체 제어 상태를 결정합니다. 제어 상태를 결정할 때 Security Hub CSPM은 ARCHIVED가 RecordState인 조사 결과와 Workflow.Status이 SUPPRESSED인 조사 결과를 무시합니다.

제어 상태에는 다음 값 중 하나가 할당됩니다.

- 통과 - 모든 조사 결과가 PASSED의 준수 상태임을 나타냅니다.
- 실패 - 하나 이상의 결과 FAILED의 준수 상태임을 나타냅니다.
- 알 수 없음 - 하나 이상의 결과가 WARNING 또는 NOT_AVAILABLE의 준수 상태임을 나타냅니다. 규정 준수 상태가 FAILED인 조사 결과가 없습니다.
- 데이터 없음 - 제어에 대한 조사 결과가 없음을 나타냅니다. 예를 들어, 새롭게 활성화된 제어는 Security Hub CSPM이 이에 대한 조사 결과를 생성하기 시작할 때까지 이 상태를 유지합니다. 또한 모든 조사 결과가 SUPPRESSED이거나 현재 AWS 리전에서 사용할 수 없는 경우에도 제어가 이 상태에 있습니다.

- 비활성화 - 현재 계정 및 리전에서 제어가 비활성화되었음을 나타냅니다. 현재 이 계정과 리전의 이 제어에 대해 보안 검사가 수행되고 있지 않습니다. 그러나 비활성화된 제어의 조사 결과는 비활성화 후 최대 24시간 동안 준수 상태의 값을 가질 수 있습니다.

관리자 계정의 경우, 제어 상태는 관리자 계정 및 멤버 계정의 제어 상태를 반영합니다. 특히 제어의 전체 상태는 제어에 관리자 계정 또는 멤버 계정에서 하나 이상의 실패 조사 결과가 있는 경우, 실패로 표시됩니다. 집계 리전을 설정한 경우, 집계 리전의 제어 상태는 집계 리전 및 연결된 리전의 제어 상태를 반영합니다. 특히, 제어에 하나 이상의 계정과 하나의 연결된 리전에서 하나 이상의 실패한 조사 결과가 있는 경우, 제어의 전체 상태는 실패 표시됩니다.

Security Hub CSPM은 일반적으로 Security Hub CSPM 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 초기 제어 상태를 생성합니다. 또한 제어 상태가 표시되려면 AWS Config 리소스 기록이 구성되어 있어야 합니다. 제어 상태가 처음으로 생성된 후 Security Hub CSPM은 이전 24시간 동안의 조사 결과를 기반으로 24시간마다 제어 상태를 업데이트합니다. 제어 세부 정보 페이지의 타임스탬프는 제어 상태가 마지막으로 업데이트된 시간을 나타냅니다.

> **Note**
>
> 제어를 처음 활성화하면, 중국 리전 및 AWS GovCloud (US) Region에서 제어 상태가 생성되려면 최대 24시간이 소요될 수 있습니다.

## 보안 점수 계산

AWS Security Hub CSPM 콘솔의 요약 페이지와 제어 페이지에는 활성화된 모든 표준에 대한 요약 보안 점수가 표시됩니다. 또한 보안 표준 페이지에서 Security Hub CSPM은 활성화된 각 표준에 대해 0~100%의 보안 점수를 표시합니다.

Security Hub CSPM을 처음 활성화하면 Security Hub CSPM은 사용자가 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 요약 보안 점수와 표준 보안 점수를 계산합니다. 점수는 콘솔에서 해당 페이지를 방문할 때 활성화된 표준에 대해서만 생성됩니다. 또한 점수가 표시되도록 AWS Config 리소스 기록을 구성해야 합니다. 요약 보안 점수는 표준 보안 점수의 평균입니다. 현재 활성화된 표준의 목록을 검토하려면 Security Hub CSPM API의 GetEnabledStandards 작업을 사용할 수 있습니다.

Security Hub CSPM은 점수를 처음 생성한 후 24시간마다 보안 점수를 업데이트합니다. Security Hub CSPM은 보안 점수가 마지막으로 업데이트된 시점을 나타내는 타임스탬프를 표시합니다. 참고로 중국

리전 및 AWS GovCloud (US) Regions에 처음으로 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

통합 제어 조사 결과를 켜면 보안 점수가 업데이트되는 데 최대 24시간이 걸릴 수 있습니다. 또한 새로운 집계 리전을 활성화하거나 연결된 리전을 업데이트하면 기존 보안 점수가 재설정됩니다. Security Hub CSPM이 업데이트된 리전의 데이터를 포함하는 새로운 보안 점수를 생성하는 데 최대 24시간이 걸릴 수 있습니다.

보안 점수 계산 방법

보안 점수는 활성화된 제어에 대한 통과된 제어의 비율을 나타냅니다. 점수는 가장 가까운 정수로 반올림되거나 반내림된 백분율로 표시됩니다.

Security Hub CSPM은 활성화된 모든 표준에 대한 요약 보안 점수를 계산합니다. 또한 Security Hub CSPM은 활성화된 각 표준에 대한 보안 점수를 계산합니다. 점수 계산을 위해, 활성화된 제어에는 통과, 실패 및 알 수 없음 상태의 제어가 포함됩니다. 데이터 없음 상태인 제어는 점수 계산에서 제외됩니다.

Security Hub CSPM은 제어 상태를 계산할 때 보관된 조사 결과와 억제된 조사 결과를 무시합니다. 이는 보안 점수에 영향을 미칠 수 있습니다. 예를 들어, 제어에 대한 모든 실패 조사 결과를 숨기면 상태가 통과로 바뀌어 보안 점수를 높일 수 있습니다. 제어 상태에 대한 자세한 내용은 규정 준수 상태 및 제어 상태 평가 섹션을 참조하세요.

채점 예제:

| 표준 | 통과된 제어 | 실패한 제어 | 알 수 없는 제어 | 표준 점수 |
|---|---|---|---|---|
| AWS 기본 보안 모범 사례 v1.0.0 | 168 | 22 | 0 | 88% |
| CIS AWS 파운데이션 벤치마크 v1.4.0 | 8 | 29 | 0 | 22% |
| CIS AWS 파운데이션 벤치마크 v1.2.0 | 6 | 35 | 0 | 15% |
| NIST 특별 간행물 800-53 개정 5 | 159 | 56 | 0 | 74% |

| 표준 | 통과된 제어 | 실패한 제어 | 알 수 없는 제어 | 표준 점수 |
|---|---|---|---|---|
| PCI DSS v3.2.1 | 28 | 17 | 0 | 62% |

요약 보안 점수를 계산할 때 Security Hub CSPM은 표준 전체에서 각 제어를 한 번만 계산합니다. 예를 들어, 세 가지 활성화된 표준에 적용되는 제어를 활성화한 경우, 채점 목적상 하나의 활성화된 제어로만 계산됩니다.

이 예제에서는 활성화된 표준 전체에 걸쳐 활성화된 제어의 총 개수가 528개이지만 Security Hub CSPM은 채점 목적으로 각 고유 제어를 한 번만 계산합니다. 활성화된 고유한 제어의 수는 528개 미만일 수 있습니다. 활성화된 고유한 제어의 수가 515개이고 통과한 고유 제어의 수가 357개라고 가정할 경우, 요약 점수는 69% 입니다. 이 점수는 통과된 고유 제어의 수를 활성화된 고유 제어의 수로 나누어 계산합니다.

현재 리전의 계정에 하나의 표준만 활성화했더라도 요약 점수가 표준 보안 점수와 다를 수 있습니다. 관리자 계정에 로그인하고 멤버 계정에 추가 표준이나 다른 표준이 활성화되어 있는 경우, 이런 현상이 발생할 수 있습니다. 집계 영역의 점수를 보는 도중 연결된 리전에 추가 표준이나 다른 표준이 활성화되어 있는 경우에도 이런 현상이 발생할 수 있습니다.

관리자 계정의 보안 점수

관리자 계정에 로그인한 경우, 요약 보안 점수 및 표준 점수는 관리자 계정 및 모든 구성원 계정의 제어 상태를 반영합니다.

멤버 계정이 하나라도 제어 상태가 실패인 경우, 관리자 계정에서는 해당 제어의 상태가 실패로 표시되며 관리자 계정 점수에 영향을 줍니다.

관리자 계정으로 로그인하고 집계 리전에서 점수를 보는 경우, 보안 점수는 모든 구성원 계정 및 모든 연결된 리전의 제어 상태를 반영합니다.

집계 리전을 설정한 경우, 보안 점수

집계를 설정한 경우 AWS 리전요약 보안 점수 및 표준 점수는 모든의 제어 상태를 고려합니다.
연결된 리전.

하나의 연결된 리전에서라도 제어 상태가 실패인 경우, 집계 리전에서도 해당 제어의 상태가 실패로 표시되며 집계 리전 점수에 영향을 줍니다.

관리자 계정으로 로그인하고 집계 리전에서 점수를 보는 경우, 보안 점수는 모든 구성원 계정 및 모든 연결된 리전의 제어 상태를 반영합니다.

# Security Hub CSPM의 제어 범주

각 제어에는 범주가 할당됩니다. 제어 범주에는 해당 제어가 적용되는 보안 기능이 반영됩니다.

범주 값에는 범주, 범주 내의 하위 범주 및 선택적으로 하위 범주 내의 분류자가 포함됩니다. 예제:

- 식별 > 인벤토리
- 보호 > 데이터 보호 > 전송 중인 데이터 암호화

다음은 사용 가능한 범주, 하위 범주, 분류자에 대한 설명입니다.

## 식별

시스템, 자산, 데이터 및 기능에 대한 사이버 보안 위험을 관리하기 위한 조직의 이해를 높입니다.

인벤토리

서비스가 올바른 리소스 태그 지정 전략을 구현했습니까? 태그 지정 전략에 리소스 소유자가 포함됩니까?

서비스는 어떤 리소스를 사용합니까? 이 서비스에 대해 승인된 리소스가 있습니까?

승인된 인벤토리에 대한 가시성이 있습니까? 예를 들어, Amazon EC2 Systems Manager 및 Service Catalog와 같은 서비스를 사용하십니까?

로깅

서비스에 대한 모든 관련 로깅을 안전하게 활성화했습니까? 로그 파일의 예제는 다음과 같습니다.

- Amazon VPC 흐름 로그
- Elastic Load Balancing 액세스 로그
- Amazon CloudFront 로그
- Amazon CloudWatch Logs
- Amazon Relational Database Service 로깅
- Amazon OpenSearch Service 느린 인덱스 로그
- X-Ray 추적
- AWS Directory Service로그
- AWS Config항목

- 스냅샷

## 보호

중요한 인프라 서비스 및 보안 코딩 사례의 제공을 보장하기 위해 적절한 안전 장치를 개발 및 구현합니다.

보안 액세스 관리

서비스가 IAM 또는 리소스 정책에서 최소 권한 관행을 사용합니까?

암호와 보안 정보는 충분히 복잡합니까? 그들은 적절하게 교체됩니까?

서비스가 다중 인증(MFA)을 사용합니까?

서비스가 루트 사용자를 피합니까?

리소스 기반 정책에서 퍼블릭 액세스를 허용합니까?

보안 네트워크 구성

서비스가 안전하지 않은 퍼블릭 원격 네트워크 액세스를 방지합니까?

서비스가 VPC를 제대로 사용합니까? 예를 들어, 작업을 VPC에서 실행해야 합니까?

서비스가 민감한 리소스를 적절하게 분할하고 격리합니까?

데이터 보호

저장 데이터 암호화 - 서비스가 저장 데이터를 암호화합니까?

전송 중인 데이터 암호화 - 서비스가 전송 중인 데이터를 암호화합니까?

데이터 무결성 - 서비스가 데이터의 무결성을 검증합니까?

데이터 삭제 보호 - 서비스가 실수로 인한 삭제로부터 데이터를 보호합니까?

데이터 관리/사용 – Amazon Macie와 같은 서비스를 사용하여 민감한 데이터의 위치를 추적합니까?

API 보호

서비스가를 사용하여 서비스 API 작업을 AWS PrivateLink보호하나요?

보호 서비스

올바른 보호 서비스가 있습니까? 그들은 정확한 양의 범위를 제공합니까?

보호 서비스는 서비스를 대상으로 하는 공격 및 손상을 차단하는 데 도움이 됩니다. 의 보호 서비스의 예로는 AWS Control Tower,AWS WAF,AWS Shield Advanced, Vanta, Secrets Manager, IAM Access Analyzer 및 등이 AWS있습니다AWS Resource Access Manager.

안전한 개발

보안 코딩 사례를 사용합니까?

Open Web Application Security Project(OWASP) Top 10과 같은 취약점을 피합니까?

## 감지

사이버 보안 이벤트의 발생을 식별하기 위한 적절한 활동을 개발하고 구현합니다.

감지 서비스

올바른 감지 서비스가 있습니까?

그들은 정확한 양의 범위를 제공합니까?

AWS탐지 서비스의 예로는 Amazon GuardDuty,AWSSecurity Hub CSPM, Amazon Inspector, Amazon Detective, Amazon CloudWatch 경보 AWS IoT Device Defender및 등이 있습니다AWS Trusted Advisor.

## 대처

감지된 사이버 보안 이벤트와 관련하여 조치를 취할 수 있는 적절한 활동을 개발하고 구현합니다.

응답 조치

보안 이벤트에 신속하게 대응하고 있습니까?

치명적이거나 심각도가 높은 활성 조사 결과가 있습니까?

포렌식

서비스에 대한 포렌식 데이터를 안전하게 획득할 수 있습니까? 예를 들어, 진정한 긍정적인 조사 결과와 관련된 Amazon EBS 스냅샷을 확보하고 있습니까?

포렌식 계정을 설정했습니까?

### 복구

복원성 계획을 유지하고 사이버 보안 이벤트로 인해 손상된 기능이나 서비스를 복원하기 위한 적절한 활동을 개발하고 구현합니다.

복원력

서비스 구성이 정상적인 장애 조치, 탄력적 확장 및 고가용성을 지원합니까?

백업을 설정했습니까?

## Security Hub CSPM에서 제어 세부 정보 검토

Security Hub CSPM 콘솔의 제어 페이지 또는 표준 세부 정보 페이지에서 제어를 선택하면 제어 세부 정보 페이지로 이동합니다.

제어 세부 정보 페이지 상단에 제어 상태가 표시됩니다. 제어 상태는 제어 조사 결과의 규정 준수 상태를 기반으로 제어 성능을 요약합니다. Security Hub CSPM은 일반적으로 Security Hub CSPM 콘솔의 요약 페이지 또는 보안 표준 페이지를 처음 방문한 후 30분 이내에 초기 제어 상태를 생성합니다. 상태는 해당 페이지를 방문할 때 활성화되는 제어에만 사용할 수 있습니다.

또한 제어 세부 정보 페이지에는 지난 24시간 동안의 제어 조사 결과의 규정 준수 상태에 대한 세부 정보가 나와 있습니다. 제어 상태 및 규정 준수 상태에 대한 자세한 내용은 규정 준수 상태 및 제어 상태 평가 섹션을 참조하세요.

AWS Config 제어 상태가 표시되도록 리소스 기록을 구성해야 합니다. 제어 상태가 처음으로 생성된 후 Security Hub CSPM은 이전 24시간 동안의 조사 결과를 기반으로 24시간마다 제어 상태를 업데이트합니다.

관리자 계정에는 관리자 계정과 구성원 계정 전체의 집계된 제어 상태가 표시됩니다. 집계 영역을 설정한 경우, 제어 상태에는 연결된 모든 리전의 조사 결과가 포함됩니다. 제어 상태에 대한 자세한 내용은 the section called “규정 준수 상태 및 제어 상태” 섹션을 참조하세요.

세부 정보 페이지에서 원하는 열을 활성화/비활성화할 수도 있습니다.

> **Note**
>
> 중국 리전 및 AWS GovCloud (US) Regions에서 최초 제어 상태가 생성되는 경우 제어 활성화 후 최대 24시간이 소요될 수 있습니다.

표준 및 요구 사항 탭에는 제어를 사용할 수 있는 표준과 다양한 규정 준수 프레임워크의 제어 관련 요구 사항이 나열됩니다.

검사 탭에는 지난 24시간 동안의 제어에 대한 활성 조사 결과가 나열됩니다. 제어 조사 결과는 Security Hub CSPM이 제어에 대한 보안 검사를 실행할 때 생성되고 업데이트됩니다. 이 탭의 목록에는 보관된 조사 결과가 포함되지 않습니다.

각 검색 조사 결과에 대해 목록은 규정 준수 상태 및 관련 리소스와 같은 조사 결과 세부 정보에 대한 액세스를 제공합니다. 또한 각 조사 결과의 워크플로 상태를 설정하고 조사 결과를 사용자 지정 작업으로 전송할 수 있습니다. 자세한 내용은 제어 조사 결과 검토 및 관리 단원을 참조하십시오.

## 제어에 대한 세부 정보 보기

원하는 액세스 방법을 선택하고 다음 단계에 따라 제어의 세부 정보를 검토하세요. 세부 정보는 현재 계정 및 리전에 적용되며 다음을 포함합니다.

- 제어의 제목 및 설명.
- 실패 제어 조사 결과에 대한 문제 해결 지침 링크.
- 제어의 심각도.
- 제어의 상태

콘솔에서 제어에 대한 최근 조사 결과의 목록을 검토할 수도 있습니다. 프로그래밍 방식으로 검토하려면 Security Hub CSPM API의 GetFindings 작업을 사용하세요.

Security Hub CSPM console

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다.
3. 제어를 선택합니다.

Security Hub CSPM API

1. `ListSecurityControlDefinitions`을(를) 실행하고 하나 이상의 표준 ARN을 입력하여 해당 표준에 대한 제어 ID 목록을 가져옵니다. 표준 ARN을 가져오려면 `DescribeStandards`을(를) 실행하세요. 표준 ARN을 입력하지 않는 경우, 이 API는 모든 Security Hub CSPM 제어 ID를 반환합니다. 이 API는 이러한 기능 릴리스 이전에 존재했던 표준 기반 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

요청 예제:

```
{
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0"
}
```

2. 를 실행BatchGetSecurityControls하여 현재 AWS 계정 및에서 하나 이상의 컨트롤에 대한 세부 정보를 가져옵니다 AWS 리전.

   요청 예제:

```
{
    "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. list-security-control-definitions 명령을 실행하고 하나 이상의 표준 ARN을 입력하여 제어 ID 목록을 가져옵니다. 표준 ARN을 얻으려면 describe-standards 명령을 실행합니다. 표준 ARN을 입력하지 않는 경우, 이 명령은 모든 Security Hub CSPM 제어 ID를 반환합니다. 이 명령은 이러한 기능 릴리스 이전에 존재했던 표준 기반 제어 ID가 아니라 표준에 구애받지 않는 보안 제어 ID를 반환합니다.

```
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. batch-get-security-controls 명령을 실행하여 현재 AWS 계정 및 AWS 리전에 있는 하나 이상의 제어에 대한 세부 정보를 가져옵니다.

```
aws securityhub --region us-east-1 batch-get-security-controls --security-control-ids '["Config.1", "IAM.1"]'
```

# Security Hub CSPM에서 제어 필터링 및 정렬

AWS Security Hub CSPM 콘솔에서 제어 페이지를 사용하여 현재에서 사용할 수 있는 제어 테이블을 검토할 수 있습니다 AWS 리전. 집계 영역은 예외입니다. 집계 영역을 구성하고 해당 리전에 로그인한 경우 콘솔에 집계 영역 또는 하나 이상의 연결된 리전에서 사용할 수 있는 제어가 표시됩니다.

제어의 특정 하위 집합에 집중할 수 있도록 테이블을 필터링하고 정렬할 수 있습니다. 테이블 옆의 필터링 기준 옵션을 사용하면 다음과 같은 특정 하위 집합에 빠르게 집중할 수 있습니다.

- 모든 활성화된 제어(하나 이상의 활성화된 표준에서 활성화된 제어).
- 모든 비활성화된 제어(모든 표준에서 비활성화된 제어).
- 실패와 같이 특정 제어 상태가 있는 모든 활성화된 제어. 데이터 없음 옵션은 현재 조사 결과가 없는 제어만 표시합니다. 제어 상태에 대한 자세한 내용은 규정 준수 상태 및 제어 상태 평가 섹션을 참조하세요.

필터링 기준 옵션 외에도, 테이블 위의 제어 필터링 상자에 필터링 기준을 입력하여 테이블을 필터링할 수 있습니다. 예를 들어, 제어 ID 또는 심각도별로 필터링할 수 있습니다.

기본적으로 실패 상태의 제어가 먼저 나열되고 심각도 기준 내림차순으로 정렬됩니다. 다른 열 제목을 선택하여 정렬 순서를 변경할 수 있습니다.

> **Tip**
>
> 제어 조사 결과를 기반으로 워크플로를 자동화하는 경우, `Title` 또는 `Description` 필드 대신 `SecurityControlId` 또는 `SecurityControlArn` ASFF 필드를 필터로 사용하는 것이 좋습니다. 후자의 필드는 때때로 변경될 수 있지만 제어 ID 및 ARN은 정적 식별자입니다.

Security Hub CSPM 관리자 계정에 로그인한 경우, 활성화 제어에는 하나 이상의 멤버 계정에서 활성화된 제어가 포함됩니다. 집계 영역을 구성한 경우, 활성화된 제어에는 하나 이상의 연결된 리전에서 활성화된 제어가 포함됩니다.

활성화된 제어 옆에 있는 옵션을 선택하면 패널이 나타나고 해당 제어가 현재 활성화된 표준이 표시됩니다. 또한 제어가 현재 비활성화되어 있는 표준도 확인할 수 있습니다. 이 패널에서 제어를 모든 표준에서 비활성화할 수 있습니다. 자세한 내용은 Security Hub CSPM에서 제어 비활성화 단원을 참조하십시오. 관리자 계정의 경우, 패널에 표시된 정보는 모든 멤버 계정에 대한 설정을 반영합니다.

프로그래밍 방식으로 제어 목록을 검색하려면 Security Hub CSPM API의 ListSecurityControlDefinitions 작업을 사용할 수 있습니다. 개별 제어의 세부 정보를 검색하려면 BatchGetSecurityControls 작업을 사용합니다.

## Security Hub CSPM의 제어 파라미터 이해

AWS Security Hub CSPM의 일부 제어는 제어 평가 방식에 영향을 미치는 파라미터를 사용합니다. 일반적으로 이러한 제어는 Security Hub CSPM에서 정의하는 기본 파라미터 값을 기준으로 평가합니다. 하지만 이러한 제어의 한 하위 세트에 대해서는 파라미터 값을 수정할 수 있습니다. 제어의 파라미터 값을 사용자 지정하면 Security Hub CSPM은 지정한 값을 기준으로 제어를 평가하기 시작합니다. 제어의 기반이 되는 리소스가 사용자 지정 값을 만족하는 경우, Security Hub CSPM은 `PASSED` 조사 결과를 생성합니다. 리소스가 사용자 지정 값을 만족하지 않으면 Security Hub CSPM은 `FAILED` 조사 결과를 생성합니다.

제어 파라미터를 사용자 지정하면 Security Hub CSPM이 권장하고 모니터링하는 보안 모범 사례를 비즈니스 요구 사항 및 보안 기대치에 맞게 조정할 수 있습니다. 제어에 대한 조사 결과를 숨기는 대신 하나 이상의 파라미터를 사용자 지정하여 보안 요구 사항에 맞는 조사 결과를 얻을 수 있습니다.

다음은 사용자 지정 제어 파라미터 수정과 설정 사용자 지정 값의 몇 가지 샘플 사용 사례입니다.

- [CloudWatch.16] – CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.

  보존 기간을 지정할 수 있습니다.
- [IAM.7] – IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.

  암호 강도와 관련된 파라미터를 지정할 수 있습니다.
- [EC2.18] 보안 그룹은 승인된 포트에 대해 무제한 수신 트래픽만 허용해야 합니다.

  수신 트래픽을 제한 없이 허용할 수 있는 포트를 지정할 수 있습니다.
- [Lambda.5] - VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

  조사 결과 통과를 생성하는 최소 가용 영역 수를 지정할 수 있습니다.

이 섹션에서는 제어 파라미터를 수정할 때 고려해야 할 사항에 대해 다룹니다.

### 제어 파라미터 값 수정의 영향

파라미터 값을 변경하면 새로운 값을 기반으로 제어를 평가하는 새로운 보안 검사도 트리거됩니다. 그런 다음 Security Hub CSPM은 새로운 값을 기반으로 새로운 제어 조사 결과를 생성합니다. 제어 조사

결과를 정기적으로 업데이트하는 동안 Security Hub CSPM은 새로운 파라미터 값도 사용합니다. 제어의 파라미터 값을 변경했지만 제어가 포함된 표준을 활성화하지 않은 경우, Security Hub CSPM은 새로운 값을 사용하여 보안 검사를 수행하지 않습니다. Security Hub CSPM이 새로운 파라미터 값을 기반으로 제어를 평가하려면 관련 표준을 하나 이상 활성화해야 합니다.

제어에는 하나 이상의 사용자 지정 파라미터 설정이 있을 수 있습니다. 개별 제어 파라미터에 가능한 데이터 유형은 다음과 같습니다.

- Boolean
- 배정밀도 실수
- Enum
- EnumList
- Integer
- IntegerList
- String
- StringList

사용자 지정 파라미터 값은 활성화된 표준 전체에 적용됩니다. 현재 리전에서 지원되지 않는 제어의 파라미터는 사용자 지정할 수 없습니다. 개별 제어의 리전별 제한 목록은 Security Hub CSPM 제어에 대한 리전별 제한 섹션을 참조하세요.

일부 제어의 경우, 허용되는 파라미터 값도 지정된 범위에 속해야 유효합니다. 이러한 경우, Security Hub CSPM은 허용 가능한 범위를 제공합니다.

Security Hub CSPM은 기본 파라미터 값을 선택하고 때때로 이를 업데이트할 수 있습니다. 제어 파라미터를 사용자 지정한 후 해당 값은 변경하지 않는 한 파라미터에 대해 지정한 값이 계속 유지됩니다. 즉, 파라미터의 사용자 지정 값이 Security Hub CSPM이 정의한 현재 기본값과 일치하더라도 파라미터는 기본 Security Hub CSPM 값에 대한 업데이트 추적을 중지합니다. 다음은 [ACM.1] - 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다 제어의 예제입니다.

```
{
    "SecurityControlId": "ACM.1",
    "Parameters": {
        "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
                "Integer": 30
```

```
            }
        }
    }
}
```

위 예제에서 `daysToExpiration` 파라미터의 사용자 지정 값은 `30`입니다. 이 파라미터의 현재 기본값 또한 `30`입니다. Security Hub CSPM이 기본값을 `14`로 변경하는 경우, 이 예제의 파라미터는 해당 변경 내용을 추적하지 않습니다. 값은 `30`(으)로 유지됩니다.

파라미터의 기본 Security Hub CSPM 값에 대한 업데이트를 추적하려면 `ValueType` 필드를 `CUSTOM` 대신 `DEFAULT`로 설정하세요. 자세한 내용은 단일 계정 및 리전에서 기본 파라미터 값으로 되돌리기 단원을 참조하십시오.

## 사용자 지정 파라미터를 지원하는 제어

사용자 지정 파라미터를 지원하는 보안 제어 목록을 보려면 Security Hub CSPM 콘솔의 제어 페이지 또는 Security Hub CSPM 제어 참조 섹션을 참조하세요. 프로그래밍 방식으로 이 목록을 검색하려면 ListSecurityControlDefinitions 작업을 사용하면 됩니다. 응답에서 `CustomizableProperties` 객체는 사용자 지정 가능한 파라미터를 지원하는 제어를 나타냅니다.

## 현재 제어 파라미터 값 검토

제어 파라미터를 수정하기 전에 제어 파라미터의 현재 값을 아는 것이 도움이 될 수 있습니다.

계정에서 개별 제어 파라미터의 현재 값을 검토할 수 있습니다. 중앙 구성을 사용하는 경우 위임된 AWS Security Hub CSPM 관리자는 구성 정책에 지정된 파라미터 값도 검토할 수 있습니다.

원하는 방법을 선택하고 단계에 따라 현재 제어 파라미터 값을 검토하세요.

Security Hub CSPM console

현재 제어 파라미터 값을 검토하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다. 제어를 선택합니다.
3. 파라미터 탭을 선택합니다. 이 탭에는 제어의 현재 파라미터 값이 표시됩니다.

Security Hub CSPM API

현재 제어 파라미터 값을 검토하려면(API)

BatchGetSecurityControls API를 호출하고 하나 이상의 보안 제어 ID 또는 ARN을 제공하세요. 응답의 `Parameters` 객체에는 지정된 제어의 현재 파라미터 값이 표시됩니다.

예를 들어 다음 AWS CLI 명령은 , `APIGatway.1` `CloudWatch.15`및에 대한 현재 파라미터 값을 보여줍니다`IAM.7`. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

중앙 구성 정책에서 현재 파라미터 값을 보려면 원하는 방법을 선택하세요.

Security Hub CSPM console

구성 정책의 현재 파라미터 값을 검토하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭에서 구성 정책을 선택한 다음 세부 정보 보기를 선택합니다. 그러면 현재 파라미터 값을 포함한 정책 세부 정보가 나타납니다.

Security Hub CSPM API

구성 정책의 현재 파라미터 값을 검토하려면(API)

1. 홈 리전의 위임된 관리자 계정에서 GetConfigurationPolicy API를 호출합니다.
2. 세부 정보를 보려는 구성 정책의 ARN 또는 ID를 입력합니다. 응답에는 현재 파라미터 값이 포함됩니다.

예를 들어 다음 AWS CLI 명령은 지정된 구성 정책에서 현재 제어 파라미터 값을 검색합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub get-configuration-policy \
```

```
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

제어 조사 결과에는 제어 파라미터의 현재 값도 포함됩니다. AWS 보안 조사 결과 형식(ASFF)에서는 이러한 값이 `Compliance` 객체의 `Parameters` 필드에 표시됩니다. Security Hub CSPM 콘솔에서 조사 결과를 검토하려면 탐색 창에서 조사 결과를 선택합니다. 조사 결과를 프로그래밍 방식으로 검토하려면 Security Hub CSPM API의 GetFindings 작업을 사용하세요.

## 제어 파라미터값 사용자 지정

제어 파라미터를 사용자 지정하는 지침은 AWS Security Hub CSPM에서 중앙 구성을 사용하는지 여부에 따라 달라집니다. 중앙 구성은 위임된 Security Hub CSPM 관리자가 AWS 리전, 계정 및 조직 단위(OUs.

조직에서 중앙 구성을 사용하는 경우, 위임된 관리자는 사용자 지정 제어 파라미터가 포함된 구성 정책을 만들 수 있습니다. 이러한 정책은 중앙에서 관리되는 구성원 계정 및 OU에 연결할 수 있으며 홈 리전 및 연결된 모든 리전에 적용됩니다. 또한 위임된 관리자는 하나 이상의 계정을 자체 관리형 계정으로 지정할 수 있으며, 이렇게 하면 계정 소유자가 각 리전에서 개별적으로 자체 파라미터를 구성할 수 있습니다. 조직에서 중앙 구성을 사용하지 않는 경우, 각 계정 및 리전에서 제어 파라미터를 개별적으로 사용자 지정해야 합니다.

중앙 구성을 사용하면 조직의 여러 부분에 걸쳐 제어 파라미터 값을 조정할 수 있으므로 중앙 구성을 사용하는 것이 좋습니다. 예를 들어, 모든 테스트 계정은 특정 파라미터 값을 사용하고 모든 프로덕션 계정은 다른 값을 사용할 수 있습니다.

다중 계정 및 리전의 제어 파라미터를 사용자 지정하려면

중앙 구성을 사용하는 조직의 Security Hub CSPM 위임된 관리자인 경우, 원하는 방법을 선택하고 단계에 따라 다중 계정 및 리전의 제어 파라미터를 사용자 지정합니다.

Security Hub CSPM console

다중 계정 및 리전의 제어 파라미터 값을 사용자 지정하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.

   홈 리전에 로그인했는지 확인합니다.

2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다.
4. 사용자 지정 파라미터가 포함된 새로운 구성 정책을 만들려면 정책 생성을 선택합니다. 기존 구성 정책에서 사용자 지정 파라미터를 지정하려면 정책을 선택한 다음 편집을 선택합니다.

   사용자 지정 파라미터 값을 사용하여 새로운 구성 정책을 만들려면

   1. 사용자 지정 정책 섹션에서 활성화하려는 보안 표준 및 제어를 선택합니다.
   2. 제어 파라미터 사용자 지정을 선택합니다.
   3. 제어를 선택한 다음 하나 이상의 파라미터에 대한 사용자 지정 값을 지정합니다.
   4. 더 많은 제어에 사용할 파라미터를 사용자 지정하려면 추가 제어 사용자 지정을 선택합니다.
   5. 계정 섹션에서 정책을 적용할 계정 또는 OU를 선택합니다.
   6. 다음을 선택합니다.
   7. 정책 생성 및 적용을 선택합니다. 홈 리전 및 연결된 모든 리전에서 이 작업은 이 구성 정책과 연결된 계정 및 OU의 기존 구성 설정보다 우선합니다. 계정과 OU는 상위로부터의 직접 적용 또는 상속을 통해 구성 정책에 연결할 수 있습니다.

   기존 구성 정책에서 제어 파라미터 값을 사용자 지정하려면

   1. 제어 섹션의 사용자 지정 정책에서 원하는 새로운 사용자 지정 파라미터 값을 지정합니다.
   2. 이 정책의 제어 파라미터를 처음으로 사용자 지정하는 경우, 제어 파라미터 사용자 지정을 선택한 다음 사용자 지정할 제어를 선택합니다. 더 많은 제어에 사용할 파라미터를 사용자 지정하려면 추가 제어 사용자 지정을 선택합니다.
   3. 계정 섹션에서 정책을 적용할 계정 또는 OU를 확인합니다.
   4. 다음을 선택합니다.
   5. 변경 내용을 검토하고 올바른지 확인합니다. 완료하면 정책 저장 및 적용을 선택합니다. 홈 리전 및 연결된 모든 리전에서 이 작업은 이 구성 정책과 연결된 계정 및 OU의 기존 구성 설정보다 우선합니다. 계정과 OU는 상위로부터의 직접 적용 또는 상속을 통해 구성 정책에 연결할 수 있습니다.

Security Hub CSPM API

다중 계정 및 리전의 제어 파라미터 값을 사용자 지정하려면(API)

사용자 지정 파라미터 값을 사용하여 새로운 구성 정책을 만들려면

1. 홈 리전의 위임된 관리자 계정에서 CreateConfigurationPolicy API를 호출합니다.
2. SecurityControlCustomParameters 객체에는 사용자 지정하려는 각 제어의 식별자를 입력합니다.
3. Parameters 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우, ValueType에 대해 CUSTOM을(를) 입력합니다. Value에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. ValueType이(가) CUSTOM인 경우, Value 필드를 비워둘 수 없습니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. GetSecurityControlDefinition API를 호출하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.

기존 구성 정책에서 제어 파라미터 값을 사용자 지정하려면

1. 홈 리전의 위임된 관리자 계정에서 UpdateConfigurationPolicy API를 호출합니다.
2. Identifier 필드에는 업데이트하려는 구성 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. SecurityControlCustomParameters 객체에는 사용자 지정하려는 각 제어의 식별자를 입력합니다.
4. Parameters 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우, ValueType에 대해 CUSTOM을(를) 입력합니다. Value에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다. GetSecurityControlDefinition API를 호출하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.

예를 들어 다음 AWS CLI 명령은의 daysToExpiration 파라미터에 대한 사용자 지정 값을 사용하여 새 구성 정책을 생성합니다ACM.1. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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}}}]}}}'
```

### 단일 계정 및 리전의 제어 파라미터 사용자 지정

중앙 구성을 사용하지 않거나 자체 관리형 계정이 있는 경우, 한 번에 한 리전의 계정에 대한 제어 파라미터를 사용자 지정할 수 있습니다.

원하는 방법을 선택하고 단계에 따라 제어 파라미터를 사용자 지정하세요. 변경 사항은 현재 리전의 계정에만 적용됩니다. 추가 리전의 제어 파라미터를 사용자 지정하려면 파라미터를 사용자 지정하려는 각 추가 계정 및 리전에서 다음 단계를 반복합니다. 동일한 제어가 리전마다 다른 파라미터 값을 사용할 수 있습니다.

#### Security Hub CSPM console

하나의 계정 및 리전의 제어 파라미터 값을 사용자 지정하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다. 테이블에서 사용자 지정 파라미터를 지원하고 파라미터를 변경하고자 하는 제어를 선택합니다. 사용자 지정 파라미터 열에는 사용자 지정 파라미터를 지원하는 제어가 표시됩니다.
3. 제어의 세부 정보 페이지에서 파라미터 탭을 선택한 다음 편집을 선택합니다.
4. 변경하고자 하는 파라미터를 지정합니다.
5. 변경 사유 섹션에서 파라미터를 사용자 지정하는 이유를 선택할 수도 있습니다.
6. 저장을 선택합니다.

#### Security Hub CSPM API

하나의 계정 및 리전의 제어 파라미터 값을 사용자 지정하려면(API)

1. UpdateSecurityControl API를 호출합니다.
2. `SecurityControlId`에 사용자 지정하려는 제어의 ID를 입력합니다.
3. `Parameters` 객체에는 사용자 지정하려는 각 파라미터의 이름을 입력합니다. 사용자 지정하는 각 파라미터의 경우, `ValueType`에 대해 `CUSTOM`을(를) 입력합니다. `Value`에는 파라미터의 데이터 유형과 사용자 지정 값을 제공합니다. 제어가 지원하는 파라미터를 요청에서 생략해

도 해당 파라미터는 현재 값을 유지합니다. GetSecurityControlDefinition API를 호출하여 제어에 지원되는 파라미터, 데이터 유형 및 유효한 값을 찾을 수 있습니다.

4. 필요에 따라 `LastUpdateReason`에서 제어 파라미터를 사용자 지정하는 이유를 입력합니다.

예를 들어 다음 AWS CLI 명령은의 `daysToExpiration` 파라미터에 대한 사용자 지정 값을 정의합니다`ACM.1`. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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"
```

## 기본 제어 파라미터 값으로 되돌리기

제어 파라미터는 AWS Security Hub CSPM이 정의하는 기본값을 가질 수 있습니다. 가끔, Security Hub CSPM이 파라미터의 기본값을 업데이트하여 진화하는 보안 모범 사례를 반영할 수 있습니다. 제어 파라미터에 사용자 지정 값을 지정하지 않은 경우, 제어는 해당 업데이트를 자동으로 추적하고 새로운 기본값을 사용합니다.

제어의 기본 파라미터 값을 사용하도록 되돌릴 수 있습니다. 되돌리기 지침은 Security Hub CSPM에서 중앙 구성을 사용하는지 여부에 따라 달라집니다. 중앙 구성은 위임된 Security Hub CSPM 관리자가 AWS 리전, 계정 및 조직 단위(OUs.

> **Note**
>
> 모든 제어 파라미터에 Security Hub CSPM 기본값이 있는 것은 아닙니다. 이러한 경우, `ValueType`을 `DEFAULT`로 설정하면 Security Hub CSPM이 사용하는 특정 기본값이 없습니다. 대신, Security Hub CSPM은 사용자 지정 값이 없는 경우 파라미터를 무시합니다.

### 다중 계정 및 리전의 기본 제어 파라미터로 되돌리려면

중앙 구성을 사용하는 경우, 홈 계정 및 연결된 리전의 다중의 중앙 관리형 계정 및 OU에 대한 제어 파라미터를 되돌릴 수 있습니다.

원하는 방법을 선택하고 단계에 따라 중앙 구성을 사용하여 다중 계정 및 리전의 기본 파라미터 값으로 되돌리세요.

Security Hub CSPM console

다중 계정 및 리전의 기본 제어 파라미터 값으로 되돌리려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.

   홈 리전에서 위임된 Security Hub CSPM 관리자 계정의 자격 증명을 사용하여 로그인합니다.
2. 탐색 창에서 설정 및 구성을 선택합니다.
3. 정책 탭을 선택합니다.
4. 정책을 선택한 다음 편집을 선택합니다.
5. 사용자 지정 정책의 제어 섹션에는 사용자 지정 파라미터를 지정한 제어 목록이 표시됩니다.
6. 되돌릴 파라미터 값이 하나 이상 있는 제어를 찾습니다. 그런 다음 제거를 선택하여 기본값으로 되돌립니다.
7. 계정 섹션에서 정책을 적용할 계정 또는 OU를 확인합니다.
8. 다음을 선택합니다.
9. 변경 내용을 검토하고 올바른지 확인합니다. 완료하면 정책 저장 및 적용을 선택합니다. 홈 리전 및 연결된 모든 리전에서 이 작업은 이 구성 정책과 연결된 계정 및 OU의 기존 구성 설정보다 우선합니다. 계정과 OU는 상위로부터의 직접 적용 또는 상속을 통해 구성 정책에 연결할 수 있습니다.

Security Hub CSPM API

다중 계정 및 리전의 기본 제어 파라미터 값으로 되돌리려면(API)

1. 홈 리전의 위임된 관리자 계정에서 UpdateConfigurationPolicy API를 호출합니다.
2. `Identifier` 필드에는 업데이트하려는 정책의 Amazon 리소스 이름(ARN) 또는 ID를 입력합니다.
3. `SecurityControlCustomParameters` 객체에는 하나 이상의 파라미터를 되돌리려는 각 제어의 식별자를 입력합니다.
4. `Parameters` 객체에서 되돌리려는 각 파라미터에 대해 `ValueType` 필드에 `DEFAULT`을(를) 입력합니다. `ValueType`이(가) `DEFAULT`(으)로 설정된 경우, `Value` 필드에 값을 입력할 필요가 없습니다. 요청에 값이 포함된 경우, Security Hub CSPM은 해당 값을 무시합니다. 제어가 지원하는 파라미터를 요청에서 생략해도 해당 파라미터는 현재 값을 유지합니다.

> **Warning**
>
> `SecurityControlCustomParameters` 필드에서 제어 객체를 생략하면 Security Hub CSPM은 제어에 대한 모든 사용자 지정 파라미터를 기본값으로 되돌립니다. `SecurityControlCustomParameters`의 목록이 완전히 비어 있으면 모든 제어의 사용자 지정 파라미터를 기본값으로 되돌립니다.

예를 들어 다음 AWS CLI 명령은에 대한 `daysToExpiration` 제어 파라미터를 지정된 구성 정책의 기본값`ACM.1`으로 되돌립니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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"}}}]}}'
```

단일 계정 및 리전에서 기본 파라미터 값으로 되돌리기

중앙 구성을 사용하지 않거나 자체 관리형 계정이 있는 경우, 한 번에 한 리전의 계정에 대한 기본 파라미터 값을 사용하도록 되돌릴 수 있습니다.

원하는 방법을 선택하고 단계에 따라 단일 리전 계정의 기본 파라미터 값으로 되돌리세요. 추가 리전의 기본 파라미터 값으로 되돌리려면 각 추가 리전에서 이 단계를 반복하세요.

> **Note**
>
> Security Hub CSPM을 비활성화하면 사용자 지정 제어 파라미터가 재설정됩니다. 나중에 Security Hub CSPM을 다시 활성화하면 모든 제어가 기본 파라미터 값을 사용하여 시작합니다.

Security Hub CSPM console

하나의 계정 및 리전의 기본 제어 파라미터 값으로 되돌리려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 제어를 선택합니다. 기본 파라미터 값으로 재설정할 제어를 선택합니다.
3. `Parameters` 탭에서 제어 파라미터 옆의 사용자 지정을 선택합니다. 그런 다음 사용자 지정 제거를 선택합니다. 이제 이 파라미터는 기본 Security Hub CSPM 값을 사용하며 기본값에 대한 향후 업데이트를 추적합니다.
4. 되돌리려는 각 파라미터 값에 대해 이전 단계를 반복합니다.

Security Hub CSPM API

하나의 계정 및 리전의 기본 제어 파라미터 값으로 되돌리려면(API)

1. UpdateSecurityControl API를 호출합니다.
2. `SecurityControlId`에서 파라미터를 되돌리려는 제어의 ARN 또는 ID를 입력합니다.
3. `Parameters` 객체에서 되돌리려는 각 파라미터에 대해 `ValueType` 필드에 `DEFAULT`을(를) 입력합니다. `ValueType`이(가) `DEFAULT`(으)로 설정된 경우, `Value` 필드에 값을 입력할 필요가 없습니다. 요청에 값이 포함된 경우, Security Hub CSPM은 해당 값을 무시합니다.
4. 필요에 따라 `LastUpdateReason`에서 기본 파라미터 값으로 되돌릴 이유를 입력합니다.

예를 들어 다음 AWS CLI 명령은에 대한 `daysToExpiration` 제어 파라미터를 기본값`ACM.1`으로 되돌립니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \
```

```
--last-update-reason "New internal requirement"
```

### 제어 파라미터 변경 상태 확인

제어 파라미터를 사용자 지정하거나 기본값으로 되돌리려고 할 때 원하는 변경 사항이 효과적인지 확인할 수 있습니다. 이렇게 하면 제어가 예상대로 작동하고 의도한 보안 가치를 제공할 수 있습니다. 파라미터 업데이트가 실패하는 경우, Security Hub CSPM은 파라미터의 현재 값을 유지합니다.

파라미터 업데이트가 성공했는지 확인하려면 Security Hub CSPM 콘솔에서 제어의 세부 정보를 검토할 수 있습니다. 콘솔의 탐색 창에서 제어를 선택합니다. 그런 다음 컨트롤을 선택하여 세부 정보를 표시합니다. 파라미터 탭은 파라미터의 변경 상태를 보여줍니다.

프로그래밍 방식으로, 파라미터 업데이트 요청이 유효한 경우, BatchGetSecurityControls 작업에 대한 응답으로 `UpdateStatus` 필드 값은 `UPDATING`입니다. 즉, 업데이트는 유효했지만 업데이트된 파라미터 값이 아직 모든 조사 결과에 포함되어 있지 않을 수 있습니다. `UpdateState`의 값이 `READY`로 변경되면 Security Hub CSPM은 제어의 보안 검사를 실행할 때 업데이트된 제어 파라미터 값을 사용합니다. 조사 결과에는 업데이트된 파라미터 값이 포함됩니다.

이 `UpdateSecurityControl` 작업은 잘못된 파라미터 값에 대한 `InvalidInputException` 응답을 반환합니다. 응답은 실패 이유에 대한 추가 세부 정보를 제공합니다. 예를 들어, 파라미터의 유효 범위를 벗어나는 값을 지정했을 수 있습니다. 또는 올바른 데이터 유형을 사용하지 않는 값을 지정했을 수 있습니다. 올바른 입력과 함께 요청을 다시 제출하세요.

파라미터 값을 업데이트하려고 할 때 내부 오류가 발생하면 Security Hub CSPM은 AWS Config 활성화한 경우 자동으로 재시도합니다. 자세한 내용은 활성화 및 구성 전 고려 사항 AWS Config 단원을 참조하십시오.

## Security Hub CSPM에서 제어 조사 결과 검토 및 관리

제어 세부 정보 페이지에는 제어에 대한 활성 조사 결과 목록이 표시됩니다. 이 목록에는 보관된 조사 결과가 포함되어 있지 않습니다.

제어 세부 정보 페이지는 리전 간 집계를 지원합니다. 집계 영역을 설정한 경우, 제어 세부 정보 페이지의 제어 상태 및 보안 검사 목록에는 연결된 모든 AWS 리전의 검사가 포함됩니다.

이 목록은 조사 결과를 필터링하고 정렬하는 도구를 제공하므로 더 긴급한 조사 결과에 먼저 집중할 수 있습니다. 조사 결과에는 관련 서비스 콘솔의 리소스 세부 정보로 연결되는 링크가 포함될 수 있습니다. AWS Config규칙을 기반으로 하는 제어의 경우 규칙에 대한 세부 정보를 볼 수 있습니다.

AWSSecurity Hub CSPM API를 사용하여 조사 결과 및 조사 결과 세부 정보 목록을 검색할 수도 있습니다.

자세한 내용은 조사 결과 세부 정보 및 기록 검토 단원을 참조하십시오.

제어 조사 결과의 조사의 현재 상태를 반영하려면 워크플로 상태를 설정합니다. 자세한 내용은 the section called “조사 결과에 대한 워크플로 상태 설정” 단원을 참조하십시오.

또한 선택한 Security Hub CSPM 조사 결과를 Amazon EventBridge의 사용자 지정 작업으로 전송할 수도 있습니다. 자세한 내용은 the section called “사용자 지정 작업에 조사 결과 전송” 단원을 참조하십시오.

주제

- 제어 조사 결과 필터링 및 정렬
- 제어 조사 결과 샘플

## 제어 조사 결과 필터링 및 정렬

AWSSecurity Hub CSPM 콘솔의 제어 페이지 또는 표준의 세부 정보 페이지에서 제어를 선택하면 제어 세부 정보 페이지로 이동합니다.

제어 세부 정보 페이지에는 제어의 제목과 설명, 전체 제어 상태 및 지난 24시간 동안의 제어에 대한 보안 검사 내역이 표시됩니다.

제어 검사 목록 옆의 필터링 기준 옵션을 사용하여 특정 워크플로 상태 또는 규정 준수 상태 가 있는 조사 결과에 빠르게 초점을 맞춥니다.

필터 기준 옵션 외에도 필터 추가 상자를 사용하여 AWS 계정ID 또는 리소스 ID와 같은 다른 필드를 기준으로 검사 목록을 필터링할 수 있습니다.

기본적으로 규정 준수 상태가 통과인 조사 결과가 먼저 나열됩니다. 열 헤더에서 다른 옵션을 선택하여 기본 정렬을 변경할 수 있습니다.

제어 세부 정보 페이지에서 다운로드를 선택하여 제어 조사 결과의 현재 페이지를 .csv 파일로 다운로드할 수 있습니다.

조사 결과 목록을 필터링하면 필터와 일치하는 제어만 다운로드에 포함됩니다. 목록에서 특정 조사 결과를 선택하면 선택한 조사 결과만 다운로드에 포함됩니다.

조사 결과 필터링에 대한 자세한 내용은 Security Hub CSPM에서 조사 결과 필터링 섹션을 참조하세요.

# 제어 조사 결과 샘플

다음 샘플은 AWSSecurity Hub CSPM 제어 조사 결과의 예를 AWSSecurity Finding 형식(ASFF)으로 제공합니다. 제어 조사 결과의 내용은 통합 제어 조사 결과를 활성화했는지 여부에 따라 달라집니다.

통합 제어 조사 결과를 활성화하면 Security Hub CSPM은 제어가 여러 활성화된 표준에 포함되어 있더라도 제어에 대한 단일 조사 결과를 생성합니다. 이 기능을 활성화하지 않으면 Security Hub CSPM은 제어가 적용되는 활성화된 표준 각각에 대해 별도의 제어 조사 결과를 생성합니다. 예를 들어 2개의 표준을 활성화하고 두 표준 모두에 제어가 적용되는 경우 각 표준에 대해 하나씩 2개의 개별 제어 조사 결과를 수신하게 됩니다. 통합 제어 조사 결과를 활성화하면 해당 제어에 대해 하나의 조사 결과만 수신됩니다. 자세한 내용은 통합 제어 조사 결과 단원을 참조하십시오.

이 페이지의 샘플은 두 시나리오 모두의 예를 제공합니다. 샘플에는 통합 제어 조사 결과가 비활성화된 경우 개별 Security Hub CSPM 표준에 대한 제어 조사 결과와 통합 제어 조사 결과가 활성화된 경우 여러 Security Hub CSPM 표준에 대한 제어 조사 결과가 포함됩니다.

제어 조사 결과 샘플

- AWS기본 보안 모범 사례 표준에 대한 샘플 조사 결과
- CIS AWS파운데이션 벤치마크 v5.0.0에 대한 샘플 조사 결과
- CIS AWS파운데이션 벤치마크 v3.0.0에 대한 샘플 조사 결과
- CIS AWS파운데이션 벤치마크 v1.4.0에 대한 샘플 조사 결과
- CIS AWS파운데이션 벤치마크 v1.2.0에 대한 샘플 조사 결과
- NIST SP 800-53 개정 5 표준에 대한 샘플 조사 결과
- NIST SP 800-171 개정 2 표준에 대한 샘플 조사 결과
- PCI DSS v3.2.1에 대한 샘플 조사 결과
- AWS리소스 태그 지정 표준에 대한 샘플 조사 결과
- AWS Control Tower서비스 관리형 표준에 대한 샘플 조사 결과
- 여러 표준에 대한 샘플 통합 조사 결과

> **Note**
>
> 제어 조사 결과는 중국 리전 및 AWS GovCloud (US) 리전의 다양한 필드 및 값을 참조합니다. 자세한 내용은 ASFF 필드 및 값에 대한 통합의 영향 단원을 참조하십시오.

### AWS기본 보안 모범 사례 표준에 대한 샘플 조사 결과

다음 샘플은 AWS 기본 보안 모범 사례(FSBP) 표준에 적용되는 제어에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.


```
{
  "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"
    ]
  }
}
```

CIS AWS파운데이션 벤치마크 v5.0.0에 대한 샘플 조사 결과

다음 샘플은 CIS AWSFoundations Benchmark v5.0.0에 적용되는 컨트롤에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
  "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"
}
```

### CIS AWS파운데이션 벤치마크 v3.0.0에 대한 샘플 조사 결과

다음 샘플은 CIS AWSFoundations Benchmark v3.0.0에 적용되는 컨트롤에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
  "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"
}
```

### CIS AWS파운데이션 벤치마크 v1.4.0에 대한 샘플 조사 결과

다음 샘플은 CIS AWSFoundations Benchmark v1.4.0에 적용되는 컨트롤에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
  "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"
    ]
  }
}
```

### CIS AWS파운데이션 벤치마크 v1.2.0에 대한 샘플 조사 결과

다음 샘플은 CIS AWSFoundations Benchmark v1.2.0에 적용되는 컨트롤에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
  "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"
    ]
  }
}
```

### NIST SP 800-53 개정 5 표준에 대한 샘플 조사 결과

다음 샘플은 NIST SP 800-53 개정 5 표준에 적용되는 제어에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
  "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"
}
```

NIST SP 800-171 개정 2 표준에 대한 샘플 조사 결과

다음 샘플은 NIST SP 800-171 개정 2 표준에 적용되는 제어에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
```

```
  "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"
}
```

### PCI DSS v3.2.1에 대한 샘플 조사 결과

다음 샘플은 PCI DSS(지불 카드 산업 데이터 보안 표준) v3.2.1에 적용되는 제어에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
  "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"
    ]
  }
}
```

### AWS리소스 태그 지정 표준에 대한 샘플 조사 결과

다음 샘플은 AWS 리소스 태그 지정 표준에 적용되는 제어에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.

```
{
  "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"
}
```

## AWS Control Tower서비스 관리형 표준에 대한 샘플 조사 결과

다음 샘플은 AWS Control Tower 서비스 관리형 표준에 적용되는 제어에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 비활성화되어 있습니다.


```
{
  "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"
    ]
```

```
  }
}
```

여러 표준에 대한 샘플 통합 조사 결과

다음 샘플은 여러 활성화된 표준에 적용되는 제어에 대한 조사 결과의 예를 제공합니다. 이 샘플에서는 통합 제어 조사 결과가 활성화되어 있습니다.

```
{
  "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"
}
```


# Security Hub CSPM의 통합 이해

AWS Security Hub CSPM은 AWS 서비스 지원되는 여러 타사 보안 솔루션에서 AWS Partner Network 보안 결과를 수집할 수 있습니다. 이러한 통합을 통해 AWS 환경 전반의 보안 및 규정 준수를 포괄적으로 파악할 수 있습니다. Security Hub CSPM은 통합 솔루션에서 결과를 수집하여 AWS Security Finding Format(ASFF)으로 변환합니다.

> **Important**
>
> 지원되는 제품 통합 AWS 과 타사 제품 통합의 경우 Security Hub CSPM은에 대해 Security Hub CSPM을 활성화한 후에만 생성된 결과를 수신하고 통합합니다 AWS 계정. 이 서비스는 Security Hub CSPM을 활성화하기 전에 생성된 보안 조사 결과를 소급하여 탐지하고 통합하지 않습니다.

Security Hub CSPM 콘솔의 통합 페이지에서는 사용 가능한 제품 통합 AWS 과 타사 제품 통합에 액세스할 수 있습니다. Security Hub CSPM API에는 통합을 관리하기 위한 작업도 있습니다.

통합을 사용하지 못할 수도 있습니다 AWS 리전. Security Hub CSPM 콘솔에서 현재 로그인한 리전이 통합을 지원하지 않는 경우, 콘솔의 통합 페이지에 표시되지 않습니다. 중국 리전 및에서 사용할 수 있는 통합 목록은 섹션을 AWS GovCloud (US) Regions참조하세요리전별 통합 사용 가능 여부.

AWS 서비스 및 내장 타사 통합 외에도 사용자 지정 보안 제품을 Security Hub CSPM과 통합할 수 있습니다. Security Hub CSPM API를 사용하여 이러한 제품의 조사 결과를 Security Hub CSPM으로 전송할 수 있습니다. API를 사용하여 Security Hub CSPM이 사용자 지정 보안 제품에서 수신한 기존 조사 결과를 업데이트할 수도 있습니다.

주제


- Security Hub CSPM 통합 목록 검토
- Security Hub CSPM 통합에서 조사 결과의 흐름 활성화
- Security Hub CSPM 통합에서 조사 결과의 흐름 비활성화
- Security Hub CSPM 통합에서 조사 결과 보기
- AWS 서비스 Security Hub CSPM과의 통합
- Security Hub CSPM과 서드 파티 제품 통합
- Security Hub CSPM과 사용자 지정 제품 통합


## Security Hub CSPM 통합 목록 검토

원하는 방법을 선택하고 단계에 따라 AWS Security Hub CSPM의 통합 목록 또는 특정 통합의 세부 정보를 검토합니다.

Security Hub CSPM console

통합 옵션 및 세부 정보를 보려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. Security Hub CSPM 탐색 창에서 통합을 선택합니다.

통합 페이지에는 다른 AWS 서비스 와의 통합이 먼저 나열되고 서드 파티 제품과의 통합이 다음에 나열됩니다.

각 통합에 대해 통합 페이지는 다음 정보를 제공합니다.

- 회사의 이름
- 제품 이름
- 통합에 대한 설명
- 통합이 적용되는 범주
- 통합을 활성화하는 방법
- 통합의 현재 상태

다음 필드의 텍스트를 입력하여 목록을 필터링할 수 있습니다.

- 회사 이름
- 제품 이름
- 통합 설명
- Categories

Security Hub CSPM API

통합 옵션 및 세부 정보를 보려면(API)

통합 목록을 가져오려면 DescribeProducts 작업을 사용합니다. 를 사용하는 경우 describe-products 명령을 AWS CLI실행합니다.

특정 제품 통합에 대한 세부 정보를 검색하려면 `ProductArn` 파라미터를 사용하여 통합의 Amazon 리소스 이름(ARN)을 지정합니다.

예를 들어 다음 AWS CLI 명령은 Security Hub CSPM과 3CORESec의 통합에 대한 세부 정보를 검색합니다.

```
$ aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

## Security Hub CSPM 통합에서 조사 결과의 흐름 활성화

AWS Security Hub CSPM 콘솔의 통합 페이지에서 각 통합을 활성화하는 데 필요한 단계를 확인할 수 있습니다.

대부분의 다른 통합에서 통합 AWS 서비스을 활성화하는 데 필요한 유일한 단계는 다른 서비스를 활성화하는 것입니다. 통합 정보에는 서비스 홈 페이지에 대한 링크가 포함됩니다. 다른 서비스를 활성화하

면 Security Hub CSPM이 서비스로부터 조사 결과를 수신할 수 있는 리소스 수준 권한이 자동으로 생성되어 적용됩니다.

타사 제품 통합의 경우에서 통합을 구매한 AWS Marketplace다음 통합을 구성해야 할 수 있습니다. 통합 정보는 이러한 태스크를 수행할 수 있는 링크를 제공합니다.

에서 둘 이상의 제품 버전을 사용할 수 있는 경우 구독하려는 AWS Marketplace버전을 선택한 다음 구독 계속을 선택합니다. 예를 들어 일부 제품은 표준 버전과 AWS GovCloud (US) 버전을 제공합니다.

제품 통합을 활성화하면 리소스 정책이 자동으로 해당 제품 구독에 연결됩니다. 이 리소스 정책은 Security Hub CSPM이 해당 제품에서 조사 결과를 수신하는 데 필요한 권한을 정의합니다.

통합을 활성화하기 위한 예비 단계를 완료한 후 해당 통합의 조사 결과 흐름을 비활성화하고 다시 활성화할 수 있습니다. 통합 페이지에서 조사 결과를 전송하는 통합의 경우, 상태 정보가 현재 조사 결과를 수락하고 있는지 여부를 표시합니다.

Security Hub CSPM console

통합에서 조사 결과의 흐름 활성화(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. Security Hub CSPM 탐색 창에서 통합을 선택합니다.
3. 조사 결과를 전송하는 통합의 경우, 상태 정보는 Security Hub CSPM이 현재 해당 통합에서 조사 결과를 수락하고 있는지 여부를 표시합니다.
4. 결과 수락을 선택합니다.

Security Hub CSPM API

EnableImportFindingsForProduct 작업을 사용합니다. 를 사용하는 경우 enable-import-findings-for-product 명령을 AWS CLI실행합니다. 통합에서 조사 결과를 수신하기 위해 Security Hub를 활성화려면 제품 ARN이 필요합니다. 사용 가능한 통합에 대한 ARN을 가져오려면 DescribeProducts 작업을 사용합니다. 를 사용하는 경우를 AWS CLI실행합니다describe-products.

예를 들어 다음 AWS CLI 명령을 사용하면 Security Hub CSPM이 CrowdStrike Falcon 통합에서 결과를 수신할 수 있습니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub enable-import-findings-for product --product-arn
 "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

# Security Hub CSPM 통합에서 조사 결과의 흐름 비활성화

원하는 방법을 선택하고 단계에 따라 AWS Security Hub CSPM 통합의 결과 흐름을 비활성화합니다.

Security Hub CSPM console

통합에서 조사 결과의 흐름 비활성화(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. Security Hub CSPM 탐색 창에서 통합을 선택합니다.
3. 조사 결과를 전송하는 통합의 경우, 상태 정보는 Security Hub CSPM이 현재 해당 통합에서 조사 결과를 수락하고 있는지 여부를 표시합니다.
4. 조사 결과 수락 중지를 선택합니다.

Security Hub CSPM API

DisableImportFindingsForProduct 작업을 사용합니다. 를 사용하는 경우 disable-import-findings-for-product 명령을 AWS CLI실행합니다. 통합에서 조사 결과 흐름을 비활성화하려면 활성화된 통합에 대한 구독 ARN이 필요합니다. ARN 구독을 가져오려면 ListEnabledProductsForImport 작업을 사용합니다. 를 사용하는 경우를 AWS CLI실행합니다list-enabled-products-for-import.

예를 들어 다음 AWS CLI 명령은 CrowdStrike Falcon 통합에서 Security Hub CSPM으로의 조사 결과 흐름을 비활성화합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub disable-import-findings-for-product --product-subscription-arn
 "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/
crowdstrike-falcon"
```

# Security Hub CSPM 통합에서 조사 결과 보기

AWS Security Hub CSPM 통합에서 조사 결과를 수락하기 시작하면 Security Hub CSPM 콘솔의 통합 페이지에 통합 상태가 조사 결과 수락 중으로 표시됩니다. 통합의 조사 결과 목록을 검토하려면 조사 결과 보기를 선택합니다.

조사 결과 목록에는 워크플로 상태가 NEW 또는 NOTIFIED인 선택한 통합에 대한 활성 조사 결과가 표시됩니다.

교차 리전 집계 활성화를 활성화한 경우, 집계 영역의 목록에는 집계 영역 및 통합이 활성화된 연결된 리전에서 나온 조사 결과가 포함됩니다. Security Hub는 교차 리전 집계 활성화 구성을 기반으로 통합을 자동으로 활성화하지 않습니다.

다른 리전의 경우, 통합 조사 결과 목록에 현재 리전의 조사 결과만 포함됩니다.

교차 리전 집계를 구성하는 방법에 대한 자세한 내용은 the section called “리전 간 데이터 집계” 섹션을 참조하세요.

조사 결과 목록에서 다음 작업을 수행할 수 있습니다.

- 목록 필터 및 그룹화 변경
- 개별 조사 결과에 대한 세부 정보 보기
- 조사 결과의 워크플로 상태 업데이트
- 사용자 지정 작업에 조사 결과 전송

## AWS 서비스 Security Hub CSPM과의 통합

AWS Security Hub CSPM은 여러 다른 와의 통합을 지원합니다 AWS 서비스. 이러한 통합을 통해 AWS 환경 전반의 보안 및 규정 준수를 포괄적으로 파악할 수 있습니다.

아래에 달리 명시되지 않는 한, Security Hub CSPM 및 다른 서비스를 활성화하면 Security Hub CSPM으로 조사 결과를 전송하는 AWS 서비스 통합이 자동으로 활성화됩니다. Security Hub CSPM 조사 결과를 수신하는 통합에는 활성화를 위한 추가 단계가 필요할 수 있습니다. 더 자세히 알아보려면 각 통합에 대한 정보를 검토하세요.

일부 통합은 전혀 사용할 수 없습니다 AWS 리전. Security Hub CSPM 콘솔에서 현재 리전에서 지원되지 않는 통합은 통합 페이지에 표시되지 않습니다. 중국 리전 및에서 사용할 수 있는 통합 목록은 섹션을 AWS GovCloud (US) Regions참조하세요리전별 통합 사용 가능 여부.

### Security Hub CSPM과의 AWS 서비스 통합 개요

다음 표에서는 조사 결과를 Security Hub CSPM으로 보내거나 Security Hub CSPM에서 조사 결과를 수신하는 AWS 서비스에 대한 개요를 제공합니다.

| 통합 AWS 서비스 | Direction | |
|---|---|---|
| AWS Config | 조사 결과를 전송합니다 | |

| 통합 AWS 서비스 | Direction | |
|---|---|---|
| AWS Firewall Manager | 조사 결과를 전송합니다 | |
| Amazon GuardDuty | 조사 결과를 전송합니다 | |
| AWS Health | 조사 결과를 전송합니다 | |
| AWS Identity and Access Management Access Analyzer | 조사 결과를 전송합니다 | |
| Amazon Inspector – | 조사 결과를 전송합니다 | |
| AWS IoT Device Defender | 조사 결과를 전송합니다 | |
| Amazon Macie | 조사 결과를 전송합니다 | |
| Amazon Route 53 Resolver DNS 방화벽 | 조사 결과를 전송합니다 | |
| AWS Systems Manager 패치 관리자 | 조사 결과를 전송합니다 | |
| AWS Audit Manager | 조사 결과를 수신합니다 | |
| 채팅 애플리케이션의 Amazon Q Developer | 조사 결과를 수신합니다 | |
| Amazon Detective | 조사 결과를 수신합니다 | |
| Amazon Security Lake | 조사 결과를 수신합니다 | |
| AWS Systems Manager Explorer 및 OpsCenter | 조사 결과 수령 및 업데이트 | |
| AWS Trusted Advisor | 조사 결과를 수신합니다 | |

## AWS 서비스 Security Hub CSPM으로 조사 결과를 보내는

다음는와 AWS 서비스 통합되며 조사 결과를 Security Hub CSPM으로 전송할 수 있습니다. Security Hub CSPM은 조사 결과를 AWS Security Finding Format으로 변환합니다.

AWS Config (조사 결과 전송)

AWS Config 는 AWS 리소스 구성을 평가, 감사 및 평가할 수 있는 서비스입니다.는 AWS 리소스 구성을 AWS Config 지속적으로 모니터링 및 기록하고 원하는 구성에 대해 기록된 구성의 평가를 자동화할 수 있습니다.

와의 통합을 사용하면 Security Hub CSPM에서 AWS Config 관리형 및 사용자 지정 규칙 평가 결과를 조사 결과로 볼 AWS Config수 있습니다. 이러한 조사 결과는 다른 Security Hub CSPM 조사 결과와 함께 볼 수 있으며, 보안 상태에 대한 포괄적인 개요를 제공합니다.

AWS Config 는 Amazon EventBridge를 사용하여 AWS Config 규칙 평가를 Security Hub CSPM으로 전송합니다. Security Hub CSPM은 규칙 평가를 AWS Security Finding Format을 따르는 조사 결과로 변환합니다. 그런 다음 Security Hub CSPM은 Amazon 리소스 이름(ARN), 리소스 태그 및 생성 날짜 등 영향을 받는 리소스에 대한 추가 정보를 수집하여 BEB(best-effort basis) 방식으로 조사 결과를 보강합니다.

이 통합에 대한 자세한 내용은 다음 섹션을 참조하세요.

가 Security Hub CSPM에 조사 결과를 AWS Config 보내는 방법

Security Hub CSPM의 모든 조사 결과는 표준 JSON 형식의 ASFF를 사용합니다. ASFF에는 결과의 출처, 영향을 받는 리소스 및 결과의 현재 상태에 대한 세부 정보가 포함됩니다.는 EventBridge를 통해 관리형 및 사용자 지정 규칙 평가를 Security Hub CSPM으로 AWS Config 보냅니다. Security Hub CSPM은 규칙 평가를 ASFF를 따르는 조사 결과로 변환하고 BEB(best-effort basis) 방식으로 조사 결과를 강화합니다.

가 Security Hub CSPM으로 AWS Config 보내는 조사 결과 유형

통합이 활성화되면는 모든 AWS Config 관리형 규칙 및 사용자 지정 규칙에 대한 평가를 Security Hub CSPM으로 AWS Config 전송합니다. Security Hub CSPM이 활성화된 후 수행된 평가만 전송됩니다. 예를 들어, AWS Config 규칙 평가에서 실패한 리소스가 5개 있다고 가정해 보겠습니다. 해당 평가 이후에 Security Hub CSPM을 활성화하고 규칙에서 실패한 6번째 리소스가 발견되면 AWS Config 는 6번째 리소스 평가만 Security Hub CSPM으로 전송합니다.

Security Hub CSPM 제어에 대한 검사를 실행하는 데 사용되는 규칙과 같은 서비스 연결 AWS Config 규칙의 평가는 제외됩니다. 단,에서를 AWS Control Tower 생성하고 관리하는 서비스 연결 규칙에 의

해 생성된 결과는 예외입니다 AWS Config. 이러한 규칙에 대한 조사 결과를 포함하면 조사 결과 데이터에에서 수행한 사전 확인 결과가 포함되도록 할 수 있습니다 AWS Control Tower.

Security Hub CSPM으로 AWS Config 조사 결과 전송

통합이 활성화되면 Security Hub CSPM은 AWS Config에서 조사 결과를 수신하는 데 필요한 권한을 자동으로 할당합니다. Security Hub CSPM은 service-to-service 수준 권한을 사용합니다. AWS Config EventBridge

조사 결과 전송 지연 시간

가 새 결과를 AWS Config 생성하면 일반적으로 5분 이내에 Security Hub CSPM에서 결과를 볼 수 있습니다.

Security Hub CSPM을 사용할 수 없을 때 다시 시도

AWS Config 는 EventBridge를 통해 최대한 조사 결과를 Security Hub CSPM에 전송합니다. 이벤트가 Security Hub CSPM에 성공적으로 전달되지 않으면 EventBridge는 최대 24시간 또는 185회 중 먼저 도래하는 시점까지 전송을 재시도합니다.

Security Hub CSPM에서 기존 AWS Config 조사 결과 업데이트

가 Security Hub CSPM에 조사 결과를 AWS Config 전송한 후 동일한 조사 결과에 대한 업데이트를 Security Hub CSPM에 전송하여 조사 결과에 대한 추가 관찰 결과를 반영할 수 있습니다. 업데이트는 `ComplianceChangeNotification` 이벤트에 대해서만 전송됩니다. 규정 준수 변경 사항이 발생하지 않으면 업데이트가 Security Hub CSPM으로 전송되지 않습니다. Security Hub CSPM은 조사 결과를 가장 최근 업데이트 이후 90일 또는 업데이트가 없는 경우, 생성일 이후 90일에 삭제됩니다.

Security Hub CSPM은 연결된 리소스를 삭제 AWS Config 하더라도에서 전송된 결과를 보관하지 않습니다.

AWS Config 조사 결과가 존재하는 리전

AWS Config 조사 결과는 리전별로 발생합니다.는 조사 결과가 발생한 동일한 리전 또는 리전의 Security Hub CSPM에 조사 결과를 AWS Config 전송합니다.

Security Hub CSPM에서 AWS Config 조사 결과 보기

AWS Config 조사 결과를 보려면 Security Hub CSPM 탐색 창에서 조사 결과를 선택합니다. 조사 결과를 필터링하여 AWS Config 조사 결과만 표시하려면 검색 창 드롭다운에서 제품 이름을 선택합니다. 구성을 입력하고 적용을 선택합니다.

## Security Hub CSPM에서 AWS Config 결과 이름 해석

Security Hub CSPM은 AWS Config 규칙 평가를를 따르는 조사 결과로 변환합니다AWS 보안 조사 결과 형식(ASFF). AWS Config 규칙 평가는 ASFF와 다른 이벤트 패턴을 사용합니다. 다음 표에는 Security Hub CSPM에서 나타나는 AWS Config 규칙 평가 필드와 ASFF 대응 필드가 매핑되어 있습니다.

| 구성 규칙 평가 조사 결과 유형 | ASFF 조사 결과 유형 | 하드코딩된 값 |
|---|---|---|
| detail.awsAccountId | AwsAccountId | |
| detail.newEvaluationResult.resultRecordedTime | CreatedAt | |
| detail.newEvaluationResult.resultRecordedTime | UpdatedAt | |
| | ProductArn | "arn:<partition>:securityhub:<region>::product/aws/config" |
| | ProductName | "Config" |
| | CompanyName | "AWS" |
| | Region | "eu-central-1" |
| configRuleArn | GeneratorId, ProductFields | |
| detail.ConfigRuleARN/finding/hash | Id | |
| detail.configRuleName | Title, ProductFields | |
| detail.configRuleName | 설명 | '이 조사 결과는 구성 규칙 (`${detail.ConfigRuleName}` )의 리소스 규정 준수 변경을 위해 작성되었습니다.' |

| 구성 규칙 평가 조사 결과 유형 | ASFF 조사 결과 유형 | 하드코딩된 값 |
|---|---|---|
| 구성 항목 'ARN' 또는 Security Hub CSPM이 계산한 ARN | Resources[i].id | |
| detail.resourceType | Resources[i].Type | "AwsS3Bucket" |
| | Resources[i].Partition | "aws" |
| | Resources[i].Region | "eu-central-1" |
| 구성 항목 "configuration" | Resources[i].Details | |
| | SchemaVersion | "2018-10-08" |
| | Severity.Label | 아래 '심각도 레이블 해석' 참조 |
| | 유형 | ["소프트웨어 및 구성 점검"] |
| detail.newEvaluationResult.complianceType | Compliance.Status | "실패함", "사용할 수 없음", "통과함" 또는 "경고" |
| | Workflow.Status | Compliance.Status가 "PASSED"로 생성되거나 Compliance.Status AWS Config 가 "FAILED"에서 "PASSED"로 변경되는 경우 "RESOLVED". 그렇지 않은 경우에는 Workflow.Status가 '새로운'이 됩니다. BatchUpdateFinds API 작업을 사용하여 이 값을 변경할 수 있습니다. |

심각도 레이블 해석

AWS Config 규칙 평가의 모든 결과에는 ASFF의 기본 심각도 레이블이 MEDIUM입니다. `BatchUpdateFindings` API 작업을 통해 조사 결과의 심각도 레이블을 업데이트할 수 있습니다.

의 일반적인 결과 AWS Config

Security Hub CSPM은 AWS Config 규칙 평가를 ASFF를 따르는 조사 결과로 변환합니다. 다음은 ASFF에서 AWS Config 의 일반적인 조사 결과의 예입니다.

> **Note**
>
> 설명이 1,024자를 초과하는 경우 1,024자로 잘리고 끝에 "(잘림)"이라고 표시됩니다.


```
{
 "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"
  ]
 }
}
```

통합 활성화 및 구성

Security Hub CSPM을 활성화하면 이 통합이 자동으로 활성화됩니다. AWS Config 는 즉시 Security Hub CSPM으로 조사 결과를 전송하기 시작합니다.

Security Hub CSPM으로의 조사 결과 게시 중지

Security Hub CSPM으로 조사 결과를 전송하는 작업을 중지하려면 Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용할 수 있습니다.

조사 결과의 흐름을 중지하는 방법에 대한 지침은 Security Hub CSPM 통합에서 조사 결과의 흐름 활성화 섹션을 참조하세요.

AWS Firewall Manager (조사 결과 전송)

Firewall Manager는 리소스에 대한 웹 애플리케이션 방화벽(WAF) 정책이나 웹 액세스 제어 목록(웹 ACL) 규칙이 규정을 준수하지 않을 경우, 조사 결과를 Security Hub CSPM으로 전송합니다. Firewall Manager는 AWS Shield Advanced 가 리소스를 보호하지 않거나 공격이 식별될 때 조사 결과를 전송합니다.

Security Hub CSPM을 활성화하면 이 통합이 자동으로 활성화됩니다. Firewall Manager는 즉시 Security Hub CSPM으로 조사 결과를 전송하기 시작합니다.

통합에 대해 자세히 알아보려면 Security Hub CSPM 콘솔의 통합 페이지를 확인하세요.

Firewall Manager에 대해 자세히 알아보려면 AWS WAF 개발자 안내서를 참조하세요.

Amazon GuardDuty(조사 결과를 전송합니다)

GuardDuty는 생성하는 모든 조사 결과 유형을 Security Hub CSPM으로 전송합니다. 일부 조사 결과 유형에는 사전 조건, 활성화 요구 사항 또는 리전 제한이 있습니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 GuardDuty 조사 결과 유형을 참조하세요.

GuardDuty의 새로운 조사 결과는 5분 이내에 Security Hub CSPM으로 전송됩니다. 조사 결과에 대한 업데이트는 GuardDuty 설정에서 Amazon EventBridge에 대해 업데이트된 조사 결과 설정을 기반으로 전송됩니다.

GuardDuty 설정 페이지를 사용하여 GuardDuty 샘플 조사 결과를 생성하면 Security Hub CSPM이 샘플 조사 결과를 수신하고 조사 결과 유형에서 접두사 `[Sample]`을 생략합니다. 예를 들어, GuardDuty `[SAMPLE] Recon:IAMUser/ResourcePermissions`의 샘플 조사 결과 유형은 Security Hub CSPM에서 `Recon:IAMUser/ResourcePermissions`로 표시됩니다.

Security Hub CSPM을 활성화하면 이 통합이 자동으로 활성화됩니다. GuardDuty는 즉시 Security Hub CSPM으로 조사 결과를 전송하기 시작합니다.

GuardDuty 통합에 대한 자세한 내용은 Amazon GuardDuty 사용 설명서의 AWS Security Hub CSPM과 통합을 참조하세요.

AWS Health (조사 결과 전송)

AWS Health 는 리소스 성능 및 AWS 서비스 및 가용성에 대한 지속적인 가시성을 제공합니다 AWS 계정. AWS Health 이벤트를 사용하여 서비스 및 리소스 변경이 AWS에서 실행 중인 애플리케이션에 어떤 영향을 미칠 수 있는지 알아볼 수 있습니다.

와의 통합은를 사용하지 AWS Health 않습니다`BatchImportFindings`. 대신 service-to-service 이벤트 메시징을 AWS Health 사용하여 조사 결과를 Security Hub CSPM으로 보냅니다.

이 통합에 대한 자세한 내용은 다음 섹션을 참조하세요.

가 Security Hub CSPM에 조사 결과를 AWS Health 보내는 방법

Security Hub CSPM에서는 보안 문제를 조사 결과와 같이 추적합니다. 일부 결과는 다른 AWS 서비스 또는 타사 파트너가 감지한 문제에서 비롯됩니다. Security Hub CSPM에는 보안 문제를 감지하고 조사 결과를 생성하는 데 사용하는 규칙 집합도 있습니다.

Security Hub CSPM은 이러한 모든 출처를 총망라하여 조사 결과를 관리할 도구를 제공합니다. 사용자는 조사 결과 목록을 조회하고 필터링할 수 있으며 주어진 조사 결과의 세부 정보를 조회할 수도 있습니다. Security Hub CSPM에서 조사 결과 세부 정보 및 기록 검토 섹션을 참조하세요. 또한 주어진 조사 결과에 대한 조사 상태를 추적할 수도 있습니다. Security Hub CSPM에서 조사 결과의 워크플로 상태 설정을(를) 참조하세요.

Security Hub CSPM의 모든 조사 결과는 AWS 보안 조사 결과 형식(ASFF)이라고 하는 표준 JSON 형식을 사용합니다. ASFF에는 문제의 출처, 영향을 받은 리소스와 조사 결과의 현재 상태 등에 관한 세부 정보가 포함됩니다.

AWS Health 는 Security Hub CSPM에 결과를 보내는 AWS 서비스 중 하나입니다.

가 Security Hub CSPM으로 AWS Health 보내는 조사 결과 유형

통합이 활성화되면는 나열된 사양 중 하나 이상을 충족하는 결과를 Security Hub CSPM으로 AWS Health 보냅니다. Security Hub CSPM은 AWS 보안 조사 결과 형식(ASFF)의 조사 결과를 수집합니다.

- AWS 서비스에 대한 다음 값 중 하나가 포함된 조사 결과:
  - `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
- AWS Health typeCode 필드에 security, abuse또는 단어certificate가 있는 결과
- AWS Health 서비스가 risk 또는 인 조사 결과 abuse

Security Hub CSPM으로 AWS Health 조사 결과 전송

조사 결과를 수락하도록 선택하면 AWS Health Security Hub CSPM은 조사 결과를 수신하는 데 필요한 권한을 자동으로 할당합니다 AWS Health. Security Hub CSPM은 service-to-service 수준 권한을 사용하여 이러한 통합을 활성화하고 사용자를 대신하여 Amazon EventBridge를 AWS Health 통해에서 결과를 가져올 수 있는 안전하고 쉬운 방법을 제공합니다. 조사 결과 수락을 선택하면 Security Hub CSPM에 AWS Health의 조사 결과를 사용할 수 있는 권한이 부여됩니다.

조사 결과 전송 지연 시간

가 새 결과를 AWS Health 생성하면 일반적으로 5분 이내에 Security Hub CSPM으로 전송됩니다.

Security Hub CSPM을 사용할 수 없을 때 다시 시도

AWS Health 는 EventBridge를 통해 최대한 결과를 Security Hub CSPM에 전송합니다. 이벤트가 Security Hub CSPM에 성공적으로 전달되지 않으면 EventBridge는 24시간 동안 이벤트 전송을 재시도합니다.

Security Hub CSPM에서 기존 조사 결과 업데이트

AWS Health 가 조사 결과를 Security Hub CSPM에 전송한 후 동일한 조사 결과에 대한 업데이트를 전송하여 조사 결과에 대한 추가 관찰 결과를 Security Hub CSPM에 반영할 수 있습니다.

조사 결과가 존재하는 리전

글로벌 이벤트의 경우는 us-east-1(AWS 파티션), cn-northwest-1(중국 파티션) 및 gov-us-west-1(GovCloud 파티션)의 Security Hub CSPM으로 조사 결과를 AWS Health 전송합니다.는 이벤트가 발생하는 동일한 리전 또는 리전의 Security Hub CSPM으로 리전별 이벤트를 AWS Health 전송합니다.

Security Hub CSPM에서 AWS Health 조사 결과 보기

Security Hub CSPM에서 AWS Health 조사 결과를 보려면 탐색 패널에서 조사 결과를 선택합니다. 조사 결과를 필터링하여 AWS Health 조사 결과만 표시하려면 제품 이름 필드에서 상태를 선택합니다.

Security Hub CSPM에서 AWS Health 결과 이름 해석

AWS Health 는를 사용하여 조사 결과를 Security Hub CSPM으로 전송합니다AWS 보안 조사 결과 형식(ASFF). AWS Health 검색은 Security Hub CSPM ASFF 형식과 다른 이벤트 패턴을 사용합니다. 아래 표에는 Security Hub CSPM에 표시되는 ASFF와 일치하는 모든 AWS Health 결과 필드가 자세히 나와 있습니다.

| 상태 조사 결과 유형 | ASFF 조사 결과 유형 | 하드코딩된 값 |
|---|---|---|
| 계정 | AwsAccountId | |
| detail.startTime | CreatedAt | |
| detail.eventDescription.latestDescription | 설명 | |
| detail.eventTypeCode | GeneratorId | |
| detail.eventArn (including account) + hash of detail.startTime | Id | |
| "arn:aws:securityhub:<region>::product/aws/health" | ProductArn | |
| account 또는 resourceId | Resources[i].id | |
| | Resources[i].Type | '기타' |
| | SchemaVersion | "2018-10-08" |
| | Severity.Label | 아래 '심각도 레이블 해석' 참고 |
| "AWS Health -" detail.eventTypeCode | 제목 | |
| - | 유형 | ["소프트웨어 및 구성 점검"] |
| event.time | UpdatedAt | |
| Health 콘솔의 이벤트 URL | SourceUrl | |

심각도 레이블 해석

ASFF 조사 결과의 심각도 레이블은 다음 논리를 사용하여 결정됩니다.

- 심각도 심각인 경우:

- AWS Health 조사 결과의 service 필드는 Risk 값을 가집니다.
- AWS Health 조사 결과의 typeCode 필드는 AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION 값을 가집니다.
- AWS Health 조사 결과의 typeCode 필드는 AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK 값을 가집니다.
- AWS Health 조사 결과의 typeCode 필드는 AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES 값을 가집니다.

심각도 높음인 경우:

- AWS Health 조사 결과의 service 필드는 Abuse 값을 가집니다.
- AWS Health 조사 결과의 typeCode 필드는 SECURITY_NOTIFICATION 값을 가집니다.
- AWS Health 조사 결과의 typeCode 필드는 ABUSE_DETECTION 값을 가집니다.

심각도 중간인 경우:

- 조사 결과의 service 필드는 ACM, ARTIFACT, AUDITMANAGER, BACKUP,CLOUDENDURE, CLOUDHSM, CLOUDTRAIL, CLOUDWATCH, CODEGURGU, COGNITO, CONFIG, CONTROLTOWER, DETECTIVE, DIRECTORYSERVICE, DRS, EVENTS, FIREWALLMANAGER, GUARDDUTY, IAM, INSPECTOR, INSPECTOR2, IOTDEVICEDEFENDER, KMS, MACIE, NETWORKFIREWALL, ORGANIZATIONS, RESILIENCEHUB, RESOURCEMANAGER, ROUTE53, SECURITYHUB, SECRETSMANAGER, SES, SHIELD, SSO 또는 WAF이 될 수 있습니다.
- AWS Health 조사 결과의 typeCode 필드는 CERTIFICATE 값을 가집니다.
- AWS Health 조사 결과의 typeCode 필드는 END_OF_SUPPORT 값을 가집니다.

의 일반적인 결과 AWS Health

AWS Health 는를 사용하여 Security Hub CSPM으로 조사 결과를 전송합니다AWS 보안 조사 결과 형식(ASFF). 다음은 일반적인 결과의 예입니다 AWS Health.

> **Note**
>
> 설명이 1024자를 초과하면 1024자에서 잘리고 끝에 (잘림) 라고 표시됩니다.

```
{
            "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"
                ]
            }
        }
    ]
}
```

통합 활성화 및 구성

Security Hub CSPM을 활성화하면 이 통합이 자동으로 활성화됩니다. AWS Health 는 즉시 Security Hub CSPM으로 조사 결과를 전송하기 시작합니다.

Security Hub CSPM으로의 조사 결과 게시 중지

Security Hub CSPM으로 조사 결과를 전송하는 작업을 중지하려면 Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용할 수 있습니다.

조사 결과의 흐름을 중지하는 방법에 대한 지침은 Security Hub CSPM 통합에서 조사 결과의 흐름 활성화 섹션을 참조하세요.

AWS Identity and Access Management Access Analyzer (조사 결과 전송)

IAM Access Analyzer를 사용하면 모든 조사 결과가 Security Hub CSPM으로 전송됩니다.

IAM 액세스 분석기는 논리 기반 추론을 통해 계정에서 지원되는 리소스에 적용되는 리소스 기반 정책을 분석합니다. IAM 액세스 분석기는 외부 보안 주체가 사용자 계정의 리소스에 액세스할 수 있도록 하는 정책 문을 감지할 때 조사 결과를 생성합니다.

IAM Access Analyzer에서는 관리자 계정만 조직에 적용되는 분석기에 대한 조사 결과를 볼 수 있습니다. 조직 분석기의 경우, `AwsAccountId` ASFF 필드는 관리자 계정 ID를 반영합니다. `ProductFields`에서 `ResourceOwnerAccount` 필드는 조사 결과가 발견된 계정을 나타냅니다. 각

계정에 대해 분석기를 개별적으로 활성화하면, Security Hub CSPM은 관리자 계정 ID를 식별하는 조사 결과와 리소스 계정 ID를 식별하는 조사 결과 등 여러 조사 결과를 생성합니다.

자세한 내용은 IAM 사용 설명서의 AWS Security Hub CSPM과의 통합을 참조하세요.

Amazon Inspector(조사 결과를 전송함)

Amazon Inspector는 AWS 워크로드에서 취약성을 지속적으로 검사하는 취약성 관리 서비스입니다. Amazon Inspector는 Amazon Elastic 컨테이너 레지스트리에 상주하는 Amazon EC2 인스턴스와 컨테이너 이미지를 자동으로 검색하고 스캔합니다. 이 검사는 소프트웨어 취약성과 의도하지 않은 네트워크 노출을 찾습니다.

Security Hub CSPM을 활성화하면 이 통합이 자동으로 활성화됩니다. Amazon Inspector는 생성한 모든 조사 결과를 즉시 Security Hub CSPM으로 전송하기 시작합니다.

통합에 대한 자세한 내용은 Amazon Inspector 사용 설명서의 AWS Security Hub CSPM과의 통합을 참조하세요.

Security Hub CSPM은 Amazon Inspector Classic에서 조사 결과를 수신할 수도 있습니다. Amazon Inspector Classic에서는 지원되는 모든 규칙 패키지에 대한 평가 실행을 통해 생성된 조사 결과를 Security Hub CSPM으로 전송합니다.

통합에 대한 자세한 내용은 Amazon Inspector Classic 사용 설명서의 AWS Security Hub CSPM과의 통합을 참조하세요.

Amazon Inspector 및 Amazon Inspector Classic의 조사 결과는 동일한 제품 ARN을 사용합니다. Amazon Inspector 조사 결과에는 `ProductFields`에 다음과 같은 항목이 있습니다.

```
"aws/inspector/ProductVersion": "2",
```

> **Note**
>
> Amazon Inspector Code Security가 생성하는 보안 조사 결과는 이 통합에 사용할 수 없습니다. 그러나 Amazon Inspector 콘솔 및 Amazon Inspector API를 통해 이러한 특정 조사 결과에 액세스할 수 있습니다.

AWS IoT Device Defender (조사 결과 전송)

AWS IoT Device Defender 는 IoT 디바이스의 구성을 감사하고, 연결된 디바이스를 모니터링하여 비정상적인 동작을 감지하고, 보안 위험을 완화하는 데 도움이 되는 보안 서비스입니다.

AWS IoT Device Defender 및 Security Hub CSPM을 모두 활성화한 후 Security Hub CSPM 콘솔의 통합 페이지를 방문하여 감사, 탐지 또는 둘 다에 대한 조사 결과 수락을 선택합니다. AWS IoT Device Defender 감사 및 탐지는 모든 조사 결과를 Security Hub CSPM으로 보내기 시작합니다.

AWS IoT Device Defender 감사는 특정 감사 검사 유형 및 감사 작업에 대한 일반 정보가 포함된 검사 요약을 Security Hub CSPM으로 전송합니다. AWS IoT Device Defender Detect는 기계 학습(ML), 통계 및 정적 동작에 대한 위반 조사 결과를 Security Hub CSPM으로 전송합니다. 또한, 감사는 Security Hub CSPM으로 조사 결과 업데이트를 전송합니다.

통합에 대한 자세한 내용은 AWS IoT 개발자 안내서의 AWS Security Hub CSPM과의 통합을 참조하세요.

Amazon Macie(조사 결과를 전송합니다)

Amazon Macie는 기계 학습과 패턴 일치를 사용하여 민감한 데이터를 검색하고, 데이터 보안 위험에 대한 가시성을 제공하며, 이러한 위험에 대한 자동 보호를 지원하는 데이터 보안 서비스입니다. Macie의 조사 결과는 Amazon S3 데이터 자산에 잠재적 정책 위반 또는 민감한 데이터가 존재함을 나타낼 수 있습니다.

Security Hub CSPM을 활성화하면 Macie는 자동으로 Security Hub CSPM으로 정책 조사 결과를 전송하기 시작합니다. 민감한 데이터 조사 결과를 Security Hub CSPM으로 전송하도록 통합을 구성할 수도 있습니다.

Security Hub CSPM에서 정책 또는 민감한 데이터 조사 결과 유형이 ASFF와 호환되는 값으로 변경됩니다. 예를 들어, Macie에서 `Policy:IAMUser/S3BucketPublic` 조사 결과 유형은 Security Hub CSPM에서 `Effects/Data Exposure/Policy:IAMUser-S3BucketPublic`으로 표시됩니다.

또한, Macie는 생성된 샘플 조사 결과를 Security Hub CSPM으로 전송합니다. 샘플 조사 결과의 경우, 영향을 받는 리소스의 이름은 `macie-sample-finding-bucket`(이)고 `Sample` 필드의 값은 `true`입니다.

자세한 내용은 Amazon Macie 사용 설명서의 Security Hub를 사용하여 Macie 조사 결과 평가를 참조하세요.

Amazon Route 53 Resolver DNS 방화벽(조사 결과 전송)

Amazon Route 53 Resolver DNS 방화벽을 사용하면 Virtual Private Cloud(VPC)의 아웃바운드 DNS 트래픽을 필터링하고 규제할 수 있습니다. 이렇게 하려면 DNS Firewall 규칙 그룹에 재사용 가능한 필터링 규칙 컬렉션을 생성하고 규칙 그룹을 VPC에 연결한 다음 DNS 방화벽 로그 및 지표 활동을 모니터링합니다. 활동에 따라 DNS Firewall 동작을 적절하게 조정할 수 있습니다. DNS Firewall은 Route 53 Resolver의 기능입니다.

Route 53 Resolver DNS Firewall은 여러 유형의 조사 결과를 Security Hub CSPM으로 전송할 수 있습니다.

- 가 관리하는 도메인 목록 AWS 인 AWS 관리형 도메인 목록과 연결된 도메인에 대해 차단되거나 경고된 쿼리와 관련된 결과입니다.
- 정의한 사용자 지정 도메인 목록과 연결된 도메인에 대해 차단 또는 경고된 쿼리와 관련된 조사 결과.
- 도메인 생성 알고리즘(DGA), DNS 터널링과 같은 고급 DNS 위협과 관련된 쿼리를 탐지할 수 있는 Route 53 Resolver 기능인 DNS Firewall Advanced에서 차단 또는 경고한 쿼리와 관련된 조사 결과.

Security Hub CSPM 및 Route 53 Resolver DNS 방화벽을 활성화하면 DNS 방화벽은 AWS 관리형 도메인 목록 및 DNS Firewall Advanced에 대한 조사 결과를 Security Hub CSPM으로 자동으로 전송하기 시작합니다. 또한 사용자 지정 도메인 목록에 대한 조사 결과를 Security Hub CSPM으로 전송하려면 Security Hub CSPM에서 통합을 수동으로 활성화합니다.

Security Hub CSPM에서 Route 53 Resolver DNS Firewall의 모든 조사 결과는 `TTPs/Impact/Impact:Runtime-MaliciousDomainRequest.Reputation` 유형입니다.

자세한 내용은 Amazon Route 53 개발자 안내서의 Route 53 Resolver DNS Firewall에서 Security Hub로 조사 결과 전송을 참조하세요.

AWS Systems Manager 패치 관리자(조사 결과 전송)

AWS Systems Manager 패치 관리자는 고객의 플릿에 있는 인스턴스가 패치 규정 준수 표준을 준수하지 않을 때 Security Hub CSPM에 조사 결과를 전송합니다.

Patch Manager는 보안 관련 업데이트와 기타 유형의 업데이트를 모두 사용하여 관리형 인스턴스를 패치하는 프로세스를 자동화합니다.

Security Hub CSPM을 활성화하면 이 통합이 자동으로 활성화됩니다. Systems Manager Patch Manager는 즉시 Security Hub CSPM으로 조사 결과를 전송하기 시작합니다.

패치 관리자 사용에 대한 자세한 내용은AWS Systems Manager 사용자 설명서의 AWS Systems Manager 패치 관리자를 참조하세요.

## AWS Security Hub CSPM에서 조사 결과를 수신하는 서비스

다음 AWS 서비스는 Security Hub CSPM과 통합되며 Security Hub CSPM으로부터 조사 결과를 받습니다. 별도로 명시되어 있는 경우, 통합 서비스는 조사 결과를 업데이트할 수도 있습니다. 이 경우, 통합 서비스에서 조사 결과를 업데이트하면 Security Hub CSPM에도 반영됩니다.

AWS Audit Manager (조사 결과 수신)

AWS Audit Manager 는 Security Hub CSPM에서 조사 결과를 수신합니다. 이러한 조사 결과는 Audit Manager 사용자가 감사를 준비하는 데 도움이 됩니다.

Audit Manager에 대한 자세한 내용은 AWS Audit Manager 사용 설명서를 참조하세요. AWSAWS Audit Manager에서 지원하는 Security Hub CSPM 검사에는 Security Hub CSPM이 Audit Manager로 조사 결과를 전송하는 제어가 나열되어 있습니다.

채팅 애플리케이션의 Amazon Q Developer(조사 결과를 수신함)

채팅 애플리케이션의 Amazon Q Developer는 Slack 채널 및 Amazon Chime 채팅방에서 AWS 리소스를 모니터링하고 상호 작용할 수 있도록 도와주는 대화형 에이전트입니다.

채팅 애플리케이션의 Amazon Q Developer는 Security Hub CSPM으로부터 조사 결과를 수신합니다.

채팅 애플리케이션의 Amazon Q Developer와 Security Hub CSPM 간 통합에 대해 자세히 알아보려면 채팅 애플리케이션의 Amazon Q Developer 관리자 안내서의 Security Hub CSPM 통합 개요를 참조하세요.

Amazon Detective(조사 결과를 수신합니다)

Detective는 AWS 리소스에서 로그 데이터를 자동으로 수집하고 기계 학습, 통계 분석 및 그래프 이론을 사용하여 더 빠르고 효율적인 보안 조사를 시각화하고 수행하는 데 도움이 됩니다.

Security Hub CSPM과 Detective의 통합을 통해 Security Hub CSPM의 Amazon GuardDuty 조사 결과를 Detective로 피벗할 수 있습니다. 그런 다음 조사 도구와 시각화를 사용하여 이 결과를 조사할 수 있습니다. 이 통합에는 Security Hub CSPM 또는 Detective에서 추가 구성이 필요하지 않습니다.

다른에서 받은 조사 결과의 경우 Security Hub CSPM 콘솔의 AWS 서비스조사 결과 세부 정보 패널에는 Detective에서 조사 하위 섹션이 포함되어 있습니다. 해당 하위 섹션에는 Detective로 연결되는 링크가 포함되어 있으며, 이 링크를 통해 조사 결과에서 보고된 보안 문제를 추가로 조사할 수 있습니다. 또한, Security Hub CSPM 조사 결과를 기반으로 Detective에서 동작 그래프를 작성하여 보다 효과적인 조사를 수행할 수 있습니다. 자세한 내용은 Amazon Detective 관리 설명서의 AWS 보안 조사 결과를 참조하세요.

교차 리전 집계가 활성화된 경우, 집계 리전에서 피벗하면 조사 결과가 발생한 리전에서 Detective가 열립니다.

링크가 작동하지 않는 경우, 문제 해결 방법은 피벗 문제 해결을 참조하세요.

Amazon Security Lake(조사 결과를 수신합니다)

Security Lake는 완전 관리형 보안 데이터 레이크 서비스입니다. Security Lake는 클라우드, 온프레미스 및 사용자 지정 소스의 보안 데이터를 계정에 저장된 데이터 레이크로 자동 중앙 집중화합니다. 구독자는 조사 및 분석 사용 사례에 Security Lake의 데이터를 사용할 수 있습니다.

이 통합을 활성화하려면 두 서비스를 모두 활성화하고 Security Lake 콘솔, Security Lake API 또는에서 Security Hub CSPM을 소스로 추가해야 합니다 AWS CLI. 이 단계를 완료하면 Security Hub CSPM이 모든 조사 결과를 Security Lake로 전송하기 시작합니다.

Security Lake는 Security Hub CSPM의 조사 결과를 자동으로 정규화하고 이를 개방형 사이버 보안 스키마 프레임워크(OCSF)로 불리는 표준화된 오픈 소스 스키마로 변환합니다. Security Lake에서 구독자를 한 명 이상 추가하여 Security Hub CSPM의 조사 결과를 사용할 수 있습니다.

Security Hub CSPM을 소스로 추가하고 구독자를 생성하는 방법에 대한 지침을 포함하여이 통합에 대한 자세한 내용은 Amazon AWS Security Lake 사용 설명서의 Security Hub CSPM과의 통합을 참조하세요.

AWS Systems Manager Explorer 및 OpsCenter(조사 결과 수신 및 업데이트)

AWS Systems Manager Explorer 및 OpsCenter는 Security Hub CSPM에서 조사 결과를 수신하고 Security Hub CSPM에서 해당 조사 결과를 업데이트합니다.

Explorer는 사용자 지정 가능한 대시보드를 제공하여 사용자의 AWS 환경에 대한 운영 상태 및 성능에 주요 인사이트와 분석을 제공합니다.

OpsCenter는 운영 작업 항목을 보고 조사하고 해결할 수 있는 중앙 위치를 제공합니다.

Explorer 및 OpsCenter에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 작업 관리를 참조하세요.

AWS Trusted Advisor (조사 결과 수신)

Trusted Advisor 는 수십만 명의 AWS 고객에게 서비스를 제공하여 학습한 모범 사례를 활용합니다.는 AWS 환경을 Trusted Advisor 검사한 다음 비용 절감, 시스템 가용성 및 성능 개선 또는 보안 격차 해소를 위한 기회가 존재할 때 권장 사항을 제시합니다.

Trusted Advisor 및 Security Hub CSPM을 모두 활성화하면 통합이 자동으로 업데이트됩니다.

Security Hub CSPM은 AWS 기본 보안 모범 사례 검사 결과를 로 전송합니다 Trusted Advisor.

Security Hub CSPM과의 통합에 대한 자세한 내용은 AWS 지원 사용 설명서의 에서 AWS Security Hub CSPM 제어 보기를 AWS Trusted Advisor Trusted Advisor참조하세요.

# Security Hub CSPM과 서드 파티 제품 통합

AWS Security Hub CSPM은 여러 타사 파트너 제품과 통합됩니다. 통합은 다음 작업 중 하나 이상을 수행할 수 있습니다.

- 생성된 조사 결과를 Security Hub CSPM으로 전송
- Security Hub CSPM으로부터 조사 결과를 수신
- Security Hub CSPM에서 조사 결과를 업데이트

조사 결과를 Security Hub CSPM으로 전송하는 통합에는 Amazon 리소스 이름(ARN)이 있습니다.

통합을 사용하지 못할 수도 있습니다 AWS 리전. Security Hub CSPM 콘솔에서 현재 로그인한 리전이 통합을 지원하지 않는 경우, 콘솔의 통합 페이지에 표시되지 않습니다. 중국 리전에서 사용할 수 있는 통합 목록은 섹션을 AWS GovCloud (US) Regions참조하세요리전별 통합 사용 가능 여부.

보안 솔루션이 있고 Security Hub CSPM 파트너가 되는 데 관심이 있다면 <securityhub-partners@amazon.com>으로 이메일을 보내주세요. 자세한 내용은 파트너 통합 가이드를 참조하세요.

## 서드 파티와 Security Hub CSPM 간 통합 개요

다음 표는 Security Hub CSPM으로 조사 결과를 전송하거나 Security Hub CSPM으로부터 조사 결과를 수신할 수 있는 서드 파티 통합의 개요를 제공합니다.

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| 3CORESec – 3CORESec NTA | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/3coresec/3coresec |
| Alert Logic – SIEMless Threat Management | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:733251395267:product/alertlogic/althreatmanagement |
| Aqua Security – Aqua Cloud Native Security Platform | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| | | /aquasecurity/aquasecurity |
| Aqua Security – Kube-bench | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/aqua-security/kube-bench |
| Armor – Armor Anywhere | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:679703615338:product/armordefense/armoranywhere |
| AttackIQ – AttackIQ | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/attackiq/attackiq-platform |
| Barracuda Networks – Cloud Security Guardian | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:151784055945:product/barracuda/cloudsecurityguardian |
| BigID – BigID Enterprise | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/bigid/bigid-enterprise |
| Blue Hexagon – Blue Hexagon forAWS | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/blue-hexagon/blue-hexagon-for-aws |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| Check Point – CloudGuard IaaS | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:758245563457:product/checkpoint/cloudguard-iaas |
| Check Point – CloudGuard Posture Management | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:634729597623:product/checkpoint/dome9-arc |
| Claroty – xDome | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/claroty/xdome |
| Cloud Storage Security – Antivirus for Amazon S3 | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/cloud-storage-security/antivirus-for-amazon-s3 |
| Contrast Security | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/contrast-security/security-assess |
| CrowdStrike – CrowdStrike Falcon | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:517716713836:product/crowdstrike/crowdstrike-falcon |
| CyberArk – Privileged Threat Analytics | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:749430749651:product/cyberark/cyberark-pta |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| Data Theorem – Data Theorem | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/data-theorem/api-cloud-web-secure |
| Drata | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/drata/drata-integration |
| Forcepoint – Forcepoint CASB | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-casb |
| Forcepoint – Forcepoint Cloud Security Gateway | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/forcepoint/forcepoint-cloud-security-gateway |
| Forcepoint – Forcepoint DLP | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-dlp |
| Forcepoint – Forcepoint NGFW | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:365761988620:product/forcepoint/forcepoint-ngfw |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| Fugue – Fugue | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/fugue/fugue |
| Guardicore – Centra 4.0 | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/guardicore/guardicore |
| HackerOne – Vulnerability Intelligence | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/hackerone/vulnerability-intelligence |
| JFrog – Xray | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/jfrog/jfrog-xray |
| Juniper Networks – vSRX Next Generation Firewall | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/juniper-networks/vsrx-next-generation-firewall |
| k9 Security – Access Analyzer | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/k9-security/access-analyzer |
| Lacework – Lacework | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/lacework/lacework |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| McAfee – MVISION Cloud Native Application Protection Platform (CNAPP) | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/mcafee-skyhigh/mcafee-mvision-cloud-aws |
| NETSCOUT – NETSCOUT Cyber Investigator | 조사 결과를 전송합니다 | arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator |
| Orca Cloud Security Platform | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/orca-security/orca-security |
| Palo Alto Networks – Prisma Cloud Compute | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:496947949261:product/twistlock/twistlock-enterprise |
| Palo Alto Networks – Prisma Cloud Enterprise | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:188619942792:product/paloaltonetworks/redlock |
| Plerion – Cloud Security Platform | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/plerion/cloud-security-platform |
| Prowler – Prowler | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/prowler/prowler |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| Qualys – Vulnerability Management | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:805950163170:product/qualys/qualys-vm |
| Rapid7 – InsightVM | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:336818582268:product/rapid7/insightvm |
| SentinelOne – SentinelOne | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/sentinelone/endpoint-protection |
| Snyk | 조사 결과를 전송합니다 | arn:aws:securityhub: *<region>*::product/snyk/snyk |
| Sonrai Security – Sonrai Dig | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/sonrai-security/sonrai-dig |
| Sophos – Server Protection | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:062897671886:product/sophos/sophos-server-protection |
| StackRox – StackRox Kubernetes Security | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/stackrox/kubernetes-security |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| Sumo Logic – Machine Data Analytics | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:956882708938:product/sumologicinc/sumologic-mda |
| Symantec – Cloud Workload Protection | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:754237914691:product/symantec-corp/symantec-cwp |
| Tenable – Tenable.io | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:422820575223:product/tenable/tenable-io |
| Trend Micro – Cloud One | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/trend-micro/cloud-one |
| Vectra – Cognito Detect | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*:978576646331:product/vectra-ai/cognito-detect |
| Wiz | 조사 결과를 전송합니다 | arn:aws:securityhub: *<REGION>*::product/wiz-security/wiz-security |
| Atlassian - Jira Service Management | 조사 결과 수신 및 업데이트 | 해당 사항 없음 |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| Atlassian - Jira Service Management Cloud | 조사 결과 수신 및 업데이트 | 해당 사항 없음 |
| Atlassian – Opsgenie | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Dynatrace | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Elastic | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Fortinet – FortiCNP | 조사 결과를 수신합니다 | 해당 사항 없음 |
| IBM – QRadar | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Logz.io Cloud SIEM | 조사 결과를 수신합니다 | 해당 사항 없음 |
| MetricStream | 조사 결과를 수신합니다 | 해당 사항 없음 |
| MicroFocus – MicroFocus Arcsight | 조사 결과를 수신합니다 | 해당 사항 없음 |
| New Relic Vulnerability Management | 조사 결과를 수신합니다 | 해당 사항 없음 |
| PagerDuty – PagerDuty | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Palo Alto Networks – Cortex XSOAR | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Palo Alto Networks – VM-Series | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Rackspace Technology – Cloud Native Security | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Rapid7 – InsightConnect | 조사 결과를 수신합니다 | 해당 사항 없음 |
| RSA – RSA Archer | 조사 결과를 수신합니다 | 해당 사항 없음 |
| ServiceNow – ITSM | 조사 결과 수신 및 업데이트 | 해당 사항 없음 |

| 통합 | Direction | ARN(해당하는 경우) |
| --- | --- | --- |
| Slack – Slack | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Splunk – Splunk Enterprise | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Splunk – Splunk Phantom | 조사 결과를 수신합니다 | 해당 사항 없음 |
| ThreatModeler | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Trellix – Trellix Helix | 조사 결과를 수신합니다 | 해당 사항 없음 |
| Caveonix – Caveonix Cloud | 조사 결과 전송 및 수신 | `arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud` |
| Cloud Custodian – Cloud Custodian | 조사 결과 전송 및 수신 | `arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian` |
| DisruptOps, Inc. – DisruptOPS | 조사 결과 전송 및 수신 | `arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops` |
| Kion | 조사 결과 전송 및 수신 | `arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio` |
| Turbot – Turbot | 조사 결과 전송 및 수신 | `arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot` |

## Security Hub CSPM으로 조사 결과를 전송하는 서드 파티 통합

다음 서드 파티 파트너 제품 통합은 Security Hub CSPM으로 조사 결과를 전송할 수 있습니다. Security Hub CSPM은 조사 결과를 AWS Security Finding Format으로 변환합니다.

3CORESec – 3CORESec NTA

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESec은(는) 온프레미스 및 AWS 시스템 모두에 대한 관리형 탐지 서비스를 제공합니다. Security Hub CSPM과의 통합을 통해 멀웨어, 권한 에스컬레이션, 수평 이동, 부적절한 네트워크 분할 등의 위협을 파악할 수 있습니다.

제품 링크

파트너 설명서

Alert Logic – SIEMless Threat Management

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

취약성 및 자산 가시성, 위협 탐지 및 인시던트 관리 AWS WAF, 할당된 SOC 분석가 옵션 등 적절한 수준의 적용 범위를 확보합니다.

제품 링크

파트너 설명서

Aqua Security – Aqua Cloud Native Security Platform

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP)은(는) CI/CD 파이프라인부터 실행 시간 프로덕션 환경에 이르기까지 컨테이너 기반 및 서버리스 애플리케이션에 대한 전체 수명 주기 보안을 제공합니다.

제품 링크

파트너 설명서

Aqua Security – Kube-bench

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench은(는) 사용자 환경에서 인터넷 보안 센터(CIS) Kubernetes Benchmark를 실행하는 오픈 소스 도구입니다.

제품 링크

파트너 설명서

Armor – Armor Anywhere

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere는에 대한 관리형 보안 및 규정 준수를 제공합니다 AWS.

제품 링크

파트너 설명서

AttackIQ – AttackIQ

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform은(는) MITRE ATT&CK 프레임워크에 따른 실제 적대적 동작을 에뮬레이션하여 전체 보안 태세를 검증하고 개선하는 데 도움이 됩니다.

제품 링크

파트너 설명서

Barracuda Networks – Cloud Security Guardian

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry은(는) 조직이 퍼블릭 클라우드에 애플리케이션을 구축하고 워크로드를 이동하는 동안 보안을 유지할 수 있도록 지원합니다.

AWS Marketplace 링크

제품 링크

BigID – BigID Enterprise

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform은(는) 기업이 모든 시스템에서 민감한 데이터(PII)를 관리하고 보호하는 데 도움이 됩니다.

제품 링크

파트너 설명서

Blue Hexagon - Blue Hexagon 용 AWS

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon은(는) 실시간 위협 탐지 플랫폼입니다. 딥 러닝 원리를 사용하여 멀웨어 및 네트워크 이상을 포함하여 알려진 위협과 알려지지 않은 위협을 탐지합니다.

AWS Marketplace 링크

파트너 설명서

Check Point – CloudGuard IaaS

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard는 클라우드의 자산을 보호 AWS 하면서 포괄적인 위협 방지 보안을 로 쉽게 확장합니다.

제품 링크

파트너 설명서

Check Point – CloudGuard Posture Management

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

검증 가능한 클라우드 네트워크 보안, 향상된 IAM 보호, 포괄적인 규정 준수와 거버넌스를 제공하는 SaaS 플랫폼입니다.

제품 링크

파트너 설명서

Claroty – xDome

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome은(는) 조직이 산업(OT), 의료(IoMT) 및 엔터프라이즈(IoT) 환경 내의 확장된 사물 인터넷(xIOT)을 통해 사이버 물리 시스템을 보호할 수 있도록 지원합니다.

제품 링크

파트너 설명서

Cloud Storage Security – Antivirus for Amazon S3

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security은(는) Amazon S3 객체에 대한 클라우드 네이티브 멀웨어 방지 및 안티바이러스 스캐닝을 제공합니다.

Antivirus for Amazon S3는 Amazon S3에 있는 객체와 파일에 대한 멀웨어 및 위협에 대한 실시간 및 예약 스캔을 제공합니다. 문제 및 감염된 파일에 대한 가시성과 해결책을 제공합니다.

제품 링크

파트너 설명서

Contrast Security – Contrast Assess

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess는 웹 앱, API 및 마이크로서비스에서 실시간 취약성 탐지를 제공하는 IAST 도구입니다. Contrast Assess는 Security Hub CSPM과 통합되어 모든 워크로드에 대한 중앙 집중식 가시성과 응답을 제공합니다.

제품 링크

파트너 설명서

CrowdStrike – CrowdStrike Falcon

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

CrowdStrike Falcon 단일 경량 센서는 차세대 안티바이러스, 엔드포인트 감지 및 응답, 클라우드를 통한 24/7 관리형 헌팅을 통합합니다.

AWS Marketplace 링크

파트너 설명서

CyberArk – Privileged Threat Analytics

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics은(는) 권한 있는 계정의 고위험 활동 및 동작을 수집, 감지하고 이에 대해 경고하고 대응하여 진행 중인 공격을 억제합니다.

제품 링크

파트너 설명서

Data Theorem – Data Theorem

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem은(는) 보안 결함과 데이터 프라이버시 격차를 찾아 웹 애플리케이션, API 및 클라우드 리소스를 지속적으로 스캔하여 AppSec 데이터 침해를 방지합니다.

제품 링크

파트너 설명서

Drata

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata은(는) SOC2, ISO, GDPR과 같은 다양한 프레임워크를 준수하고 유지할 수 있도록 지원하는 규정 준수 자동화 플랫폼입니다. Drata와 Security Hub CSPM 간의 통합을 통해 보안 조사 결과를 한 곳에서 중앙 집중화할 수 있습니다.

AWS Marketplace 링크

파트너 설명서

Forcepoint – Forcepoint CASB

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB을(를) 사용하면 클라우드 애플리케이션 사용을 검색하고, 위험을 분석하며, SaaS 및 사용자 지정 애플리케이션에 대한 적절한 제어를 적용할 수 있습니다.

제품 링크

파트너 설명서

Forcepoint – Forcepoint Cloud Security Gateway

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway은(는) 어디에 있든 사용자와 데이터에 대한 가시성, 제어 및 위협 보호를 제공하는 융합 클라우드 보안 서비스입니다.

제품 링크

파트너 설명서

Forcepoint – Forcepoint DLP

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLP은(는) 사용자가 작업하고 데이터가 상주하는 모든 곳에서 가시성과 제어 기능을 통해 사용자로 인해 발생한 위험을 해결합니다.

제품 링크

파트너 설명서

Forcepoint – Forcepoint NGFW

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFW를 사용하면 네트워크를 관리하고 위협에 대응하는 데 필요한 확장성, 보호 및 인사이트를 통해 AWS 환경을 엔터프라이즈 네트워크에 연결할 수 있습니다.

제품 링크

파트너 설명서

Fugue – Fugue

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugue은(는) 에이전트가 없고 확장 가능한 클라우드 네이티브 플랫폼으로, 동일한 정책을 사용하여 코드형 인프라 및 클라우드 런타임 환경의 지속적인 검증을 자동화합니다.

제품 링크

파트너 설명서

Guardicore – Centra 4.0

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centra은(는) 최신 데이터 센터 및 클라우드의 워크로드에 대한 흐름 시각화, 마이크로 분할 및 위반 감지 기능을 제공합니다.

제품 링크

파트너 설명서

HackerOne – Vulnerability Intelligence

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

이 HackerOne 플랫폼은 전 세계 해커 커뮤니티와 협력하여 가장 관련성이 높은 보안 문제를 찾아냅니다. Vulnerability Intelligence는 조직이 자동 스캔에서 더 나아갈 수 있도록 지원합니다. HackerOne 윤리적 해커가 검증하고 재현 단계를 제공한 취약성을 공유합니다.

AWS 마켓플레이스 링크

파트너 설명서

JFrog – Xray

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray은(는) 바이너리에서 라이선스 규정 준수 및 보안 취약성을 지속적으로 스캔하여 안전한 소프트웨어 공급망을 운영할 수 있도록 하는 범용 애플리케이션 보안 소프트웨어 구성 분석(SCA) 도구입니다.

AWS Marketplace 링크

파트너 설명서

Juniper Networks – vSRX Next Generation Firewall

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks' vSRX 가상 차세대 방화벽은 고급 보안, 안전한 SD-WAN, 강력한 네트워킹 및 내장된 자동화를 갖춘 완벽한 클라우드 기반 가상 방화벽을 제공합니다.

AWS Marketplace 링크

파트너 설명서

제품 링크

k9 Security – Access Analyzer

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security은(는) AWS Identity and Access Management 계정에 중요한 액세스 변경이 발생하면 알려줍니다. 를 사용하면 중요한 AWS 서비스 및 데이터에 대한 사용자 및 IAM 역할의 액세스를 이해할 k9 Security수 있습니다.

k9 Security은(는) 지속적인 전송을 위해 구축되었으므로 실행 가능한 액세스 감사와 AWS CDK 및 Terraform에 대한 간단한 정책 자동화를 통해 IAM을 운영할 수 있습니다.

제품 링크

파트너 설명서

Lacework – Lacework

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework은(는) 클라우드를 위한 데이터 기반 보안 플랫폼입니다. Lacework 클라우드 보안 플랫폼은 대규모 클라우드 보안을 자동화하여 빠르고 안전하게 혁신할 수 있도록 합니다.

제품 링크

파트너 설명서

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP)는 AWS 환경에 맞는 클라우드 보안 태세 관리(CSPM) 및 클라우드 워크로드 보호 플랫폼(CWPP)을 제공합니다.

제품 링크

파트너 설명서

NETSCOUT – NETSCOUT Cyber Investigator

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator은(는) 사이버 위협이 기업에 미치는 영향을 줄이는 데 도움이 되는 전사적 네트워크 위협, 위험 조사 및 포렌식 분석 플랫폼입니다.

제품 링크

파트너 설명서

Orca Cloud Security Platform

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/orca-security/orca-security`

Orca Cloud Security Platform은 전체 클라우드 자산에서 위험 및 규정 준수 문제를 식별하고, 우선순위를 정하고, 해결합니다. Orca's 에이전트리스 우선 AI 기반 플랫폼은 취약성, 잘못된 구성, 측면 이동, API 위험, 민감한 데이터, 비정상적인 이벤트 및 동작, 지나치게 허용적인 자격 증명을 탐지하는 포괄적인 적용 범위를 제공합니다.

Orca는 Security Hub CSPM과 통합되어 Security Hub CSPM에 심층적인 클라우드 보안 원격 측정을 제공합니다. Orca는 SideScanning 기술을 사용하여 클라우드 인프라, 워크로드, 애플리케이션, 데이터, API, 자격 증명 등에서 위험 우선순위를 정합니다.

제품 링크

파트너 설명서

Palo Alto Networks – Prisma Cloud Compute

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute은(는) VM, 컨테이너 및 서버리스 플랫폼을 보호하는 클라우드 네이티브 사이버 보안 플랫폼입니다.

제품 링크

파트너 설명서

Palo Alto Networks – Prisma Cloud Enterprise

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

클라우드 보안 분석, 고급 위협 탐지 및 규정 준수 모니터링을 통해 AWS 배포를 보호합니다.

제품 링크

파트너 설명서

Plerion – Cloud Security Platform

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion은(는) 워크로드 전반에 걸쳐 예방, 탐지 및 시정 조치를 제공하는 위협 중심의 고유한 위험 기반 접근 방식을 갖춘 클라우드 보안 플랫폼입니다. Plerion과 Security Hub CSPM 간의 통합을 통해 고객은 보안 조사 결과를 한 곳에서 중앙 집중화하고 조치를 취할 수 있습니다.

AWS Marketplace 링크

파트너 설명서

Prowler – Prowler

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler는 보안 모범 사례, 강화 및 지속적 모니터링과 관련된 AWS 검사를 수행하는 오픈 소스 보안 도구입니다.

제품 링크

파트너 설명서

Qualys – Vulnerability Management

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM)은(는) 취약성을 지속적으로 스캔하고 식별하여 자산을 보호합니다.

제품 링크

파트너 설명서

Rapid7 – InsightVM

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM은 최신 환경에 대한 취약성 관리 기능을 제공하므로 취약성을 효율적으로 찾고, 우선 순위를 지정하고, 문제를 해결할 수 있습니다.

제품 링크

파트너 설명서

SentinelOne – SentinelOne

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne은(는) 엔드포인트, 컨테이너, 클라우드 워크로드 및 IoT 기기 전반에서 AI 기반 예방, 탐지, 대응 및 헌팅을 포함하는 자율 확장 탐지 및 대응(XDR) 플랫폼입니다.

AWS Marketplace 링크

제품 링크

Snyk

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk은(는) AWS에서 실행 중인 워크로드의 보안 위험에 대해 앱 구성 요소를 스캔하는 보안 플랫폼을 제공합니다. 이러한 위험은 조사 결과로 Security Hub CSPM에 전송되므로 개발자와 보안 팀이 나머지 AWS 보안 조사 결과와 함께 해당 위험을 시각화하고 우선순위를 정하는 데 도움이 됩니다.

AWS Marketplace 링크

파트너 설명서

Sonrai Security – Sonrai Dig

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig은(는) 클라우드 구성 오류 및 정책 위반을 모니터링하고 수정하여 보안 및 규정 준수 태세를 개선할 수 있습니다.

제품 링크

파트너 설명서

Sophos – Server Protection

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection은(는) 포괄적인 심층 방어 기술을 사용하여 조직의 핵심 애플리케이션 및 데이터를 보호합니다.

제품 링크

StackRox – StackRox Kubernetes Security

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox은(는) 기업이 전체 컨테이너 수명 주기(구축, 배포, 실행)에 걸쳐 규정 준수 및 보안 정책을 적용하여 규모에 따라 컨테이너 및 Kubernetes 배포를 보호할 수 있도록 지원합니다.

제품 링크

파트너 설명서

Sumo Logic – Machine Data Analytics

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic은(는) 개발 및 보안 운영 팀이 AWS 애플리케이션을 구축, 실행하고 보호할 수 있게 해주는 안전한 머신 데이터 분석 플랫폼입니다.

제품 링크

파트너 설명서

Symantec – Cloud Workload Protection

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection은(는) 멀웨어 방지, 침입 방지 및 파일 무결성 모니터링을 통해 Amazon EC2 인스턴스를 완벽하게 보호합니다.

제품 링크

파트너 설명서

Tenable – Tenable.io

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

취약성을 정확하게 식별, 조사하고 우선 순위를 지정합니다. 클라우드에서 관리됩니다.

제품 링크

파트너 설명서

Trend Micro – Cloud One

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One은(는) 적절한 시기와 장소에서 팀에 적절한 보안 정보를 제공합니다. 이 통합은 보안 조사 결과를 Security Hub CSPM에 실시간으로 전송하여 Security Hub CSPM의 AWS 리소스 및 Trend Micro Cloud One 이벤트 세부 정보에 대한 가시성을 향상시킵니다.

AWS Marketplace 링크

파트너 설명서

Vectra – Cognito Detect

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectra는 고급 AI를 적용하여 숨어 있는 사이버 공격자가 도용하거나 피해를 입히기 전에 이를 감지하고 대응하여 사이버 보안을 변화시키고 있습니다.

AWS Marketplace 링크

파트너 설명서

Wiz – Wiz Security

통합 유형: 전송

제품 ARN: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz는 AWS 계정사용자, 워크로드에서 구성, 취약성, 네트워크, IAM 설정, 보안 암호 등을 지속적으로 분석하여 실제 위험을 나타내는 중요한 문제를 발견합니다. Wiz와 Security Hub CSPM을 통합하면 Security Hub CSPM 콘솔에서 Wiz가 탐지하는 문제를 시각화하고 대응할 수 있습니다.

AWS Marketplace 링크

파트너 설명서

## Security Hub CSPM으로부터 조사 결과를 수신하는 서드 파티 통합

Security Hub CSPM으로부터 조사 결과를 수신하는 서드 파티 파트너 제품 통합은 다음과 같습니다. 명시된 경우, 제품이 조사 결과를 업데이트할 수도 있습니다. 이 경우, 파트너 제품에서 수행한 조사 결과 업데이트가 Security Hub CSPM에도 반영됩니다.

Atlassian - Jira Service Management

통합 유형: 수신 및 업데이트

AWS Service Management Connector 용는 Security Hub CSPM에서 로 결과를 Jira 전송합니다Jira. Jira 문제는 결과에 따라 생성됩니다. Jira 문제가 업데이트되면 Security Hub CSPM에서 해당 조사 결과가 업데이트됩니다.

이 통합은 Jira 서버 및 Jira 데이터 센터만 지원합니다.

통합 및 작동 방식에 대한 개요는 AWS Security Hub CSPM - Atlassian Jira Service Management와(과)의 양방향 통합 동영상을 시청하세요.

제품 링크

파트너 설명서

Atlassian - Jira Service Management Cloud

통합 유형: 수신 및 업데이트

Jira Service Management Cloud은(는) Jira 서비스 관리의 클라우드 구성 요소입니다.

AWS Service Management Connector 용는 Security Hub CSPM에서 로 결과를 Jira 전송합니다 Jira. 이 조사 결과로 인해 Jira Service Management Cloud에서 문제가 발생합니다. Jira Service Management Cloud에서 이러한 문제를 업데이트하면 Security Hub CSPM에도 해당 조사 결과가 업데이트됩니다.

제품 링크

파트너 설명서

Atlassian – Opsgenie

통합 유형: 수신

Opsgenie은(는) 상시 작동 서비스를 작동하는 데 필요한 최신 인시던트 관리 솔루션으로, 개발 운영 팀이 서비스 중단에 대비하고 인시던트 발생 중 제어 유지할 수 있도록 합니다.

Security Hub CSPM과 통합하면 미션 크리티컬한 보안 관련 인시던트를 즉시 해결할 수 있도록 해당 팀으로 전달합니다.

제품 링크

파트너 설명서

Dynatrace

통합 유형: 수신

Dynatrace와 Security Hub CSPM 간 통합은 도구 및 환경 전반에서 보안 조사 결과를 통합, 시각화, 자동화하는 데 도움이 됩니다. 보안 조사 결과에 Dynatrace 런타임 컨텍스트를 추가하면 우선순위를 더 스마트하게 정하고 알림으로 인한 노이즈를 줄일 수 있으며 DevSecOps 팀이 프로덕션 환경 및 애플리케이션에 영향을 미치는 중요한 문제를 효율적으로 해결하는 데 집중할 수 있습니다.

제품 링크

파트너 설명서

Elastic

통합 유형: 수신

Elastic은 보안, 관찰성, 검색을 위한 검색 기반 솔루션을 구축합니다. Security Hub CSPM 통합을 통해 Elastic은 Security Hub CSPM의 조사 결과 및 인사이트를 프로그래밍 방식으로 수집하고, 상관관계 및

분석을 위해 이를 정규화하고, Elastic Security에 통합 대시보드 및 탐지를 표시하므로 에이전트를 배포하지 않고도 더 빠르게 분류하고 조사할 수 있습니다.

제품 링크

파트너 설명서

Fortinet – FortiCNP

통합 유형: 수신

FortiCNP은(는) 보안 조사 결과를 실행 가능한 인사이트로 집계하고 위험 점수를 기반으로 보안 인사이트의 우선 순위를 지정하여 알림으로 인한 피로를 줄이고 문제 해결을 가속화하는 클라우드 네이티브 보호 제품입니다.

AWS 마켓플레이스 링크

파트너 설명서

IBM – QRadar

통합 유형: 수신

IBM QRadar SIEM은 보안 팀이 위협을 신속하고 정확하게 감지하여 우선 순위를 정하고 조사하여 대응할 수 있는 기능을 제공합니다.

제품 링크

파트너 설명서

Logz.io Cloud SIEM

통합 유형: 수신

Logz.io은(는) 보안 팀이 보안 위협을 실시간으로 탐지, 분석 및 대응할 수 있도록 로그 및 이벤트 데이터의 고급 상관 관계를 제공하는 Cloud SIEM의 공급자입니다.

제품 링크

파트너 설명서

MetricStream – CyberGRC

통합 유형: 수신

MetricStream CyberGRC은(는) 사이버 보안 위험을 관리, 측정 및 완화하는 데 도움이 됩니다. Security Hub CSPM 조사 결과 수신하면 CyberGRC은 이러한 위험에 대한 더 많은 가시성을 제공하므로 사이버 보안 투자의 우선순위를 정하고 IT 정책을 준수할 수 있습니다.

AWS Marketplace 링크

제품 링크

MicroFocus – MicroFocus Arcsight

통합 유형: 수신

ArcSight은(는) 이벤트 상관 관계 및 감독/비감독 분석을 대응 자동화 및 오케스트레이션과 통합하여 효과적인 위협 탐지 및 대응을 실시간으로 가속화합니다.

제품 링크

파트너 설명서

New Relic Vulnerability Management

통합 유형: 수신

New Relic Vulnerability Management는 Security Hub CSPM으로부터 보안 조사 결과를 수신하므로 스택 전체에서 컨텍스트별 성능 원격 측정과 함께 보안에 대한 중앙 집중식 보기를 얻을 수 있습니다.

AWS Marketplace 링크

파트너 설명서

PagerDuty – PagerDuty

통합 유형: 수신

PagerDuty 디지털 작업 관리 플랫폼은 모든 신호를 적절한 인사이트와 조치로 자동 변환하므로 고객에게 영향을 미치는 문제를 사전에 완화할 수 있는 역량을 조직에 부여합니다.

AWS 사용자는 AWS 통합 PagerDuty 세트를 사용하여 AWS 및 하이브리드 환경을 자신 있게 확장할 수 있습니다.

체계적으로 집계된 Security Hub CSPM의 보안 경고와 통합될 경우, PagerDuty는 팀이 위협 대응 프로세스를 자동화하고 잠재적인 문제를 방지할 사용자 지정 작업을 빠르게 설정하도록 합니다.

클라우드 마이그레이션 프로젝트를 수행하는 PagerDuty 사용자는 마이그레이션 수명 주기 내내 발생하는 문제의 영향을 줄이면서 신속하게 이동할 수 있습니다.

제품 링크

파트너 설명서

Palo Alto Networks – Cortex XSOAR

통합 유형: 수신

Cortex XSOAR은(는) 전체 보안 제품 스택과 통합하여 인시던트 응답 및 보안 작업을 가속화하는 보안 오케스트레이션, 자동화 및 응답(SOAR) 플랫폼입니다.

제품 링크

파트너 설명서

Palo Alto Networks – VM-Series

통합 유형: 수신

Palo Alto VM-Series와 Security Hub CSPM 간 통합은 위협 인텔리전스를 수집하여 악의적인 IP 주소 활동을 차단하는 자동 보안 정책 업데이트로 VM-Series 차세대 방화벽에 전송합니다.

제품 링크

파트너 설명서

Rackspace Technology – Cloud Native Security

통합 유형: 수신

Rackspace Technology 은 Rackspace SOC, 고급 분석 및 위협 해결을 통한 연중무휴 모니터링을 위해 네이티브 AWS 보안 제품에 더해 관리형 보안 서비스를 제공합니다.

제품 링크

Rapid7 – InsightConnect

통합 유형: 수신

Rapid7 InsightConnect은(는) 코드를 거의 사용하지 않고 SOC 작업을 최적화할 수 있는 보안 오케스트레이션 및 자동화 솔루션입니다.

제품 링크

파트너 설명서

RSA – RSA Archer

통합 유형: 수신

RSA Archer IT 및 보안 위험 관리를 통해 비즈니스에 중요한 자산을 파악하고, 보안 정책 및 표준을 수립 및 전달하고, 공격을 탐지 및 대응하고, 보안 결함을 식별 및 해결하고, 명확한 IT 위험 관리 모범 사례를 수립할 수 있습니다.

제품 링크

파트너 설명서

ServiceNow – ITSM

통합 유형: 수신 및 업데이트

ServiceNow와 Security Hub CSPM 간 통합을 통해 ServiceNow ITSM 내에서 Security Hub CSPM의 조사 결과를 볼 수 있습니다. Security Hub CSPM으로부터 조사 결과를 수신할 때 인시던트 또는 문제를 자동으로 생성하도록 ServiceNow를 구성할 수도 있습니다.

이러한 인시던트 및 문제가 업데이트되면 Security Hub CSPM의 조사 결과도 업데이트됩니다.

통합 및 작동 방식에 대한 개요는 AWS Security Hub CSPM - ServiceNow ITSM와(과)의 양방향 통합 동영상을 시청하세요.

제품 링크

파트너 설명서

Slack – Slack

통합 유형: 수신

Slack은(는) 사람, 데이터 및 애플리케이션을 하나로 통합하는 비즈니스 기술 스택 계층입니다. 효율적으로 협업하고, 중요한 정보를 검색하고, 수십만 개의 중요한 애플리케이션 및 서비스에 액세스하여 최상의 작업을 수행할 수 있는 단일 공간입니다.

제품 링크

파트너 설명서

Splunk – Splunk Enterprise

통합 유형: 수신

Splunk는 Amazon CloudWatch Events를 Security Hub CSPM 조사 결과의 소비자로 사용합니다. 고급 보안 분석 및 SIEM을 위해 Splunk에 데이터를 보냅니다.

제품 링크

파트너 설명서

Splunk – Splunk Phantom

통합 유형: 수신

AWS Security Hub CSPM용 Splunk Phantom 애플리케이션을 사용하면 추가 위협 인텔리전스 정보로 자동화된 컨텍스트 보강을 Phantom 위해 또는 자동 대응 작업을 수행하기 위해 조사 결과가 로 전송됩니다.

제품 링크

파트너 설명서

ThreatModeler

통합 유형: 수신

ThreatModeler은(는) 엔터프라이즈 소프트웨어 및 클라우드 개발 수명 주기를 보호하고 규모를 조정하는 자동화된 위협 모델링 솔루션입니다.

제품 링크

파트너 설명서

Trellix – Trellix Helix

통합 유형: 수신

Trellix Helix은(는) 조직이 알림에서 수정까지 모든 인시던트를 제어할 수 있도록 지원하는 클라우드 호스팅 보안 운영 플랫폼입니다.

제품 링크

파트너 설명서

## Security Hub CSPM으로 조사 결과를 전송하고 Security Hub CSPM으로부터 조사 결과를 수신하는 서드 파티 통합

다음 서드 파티 파트너 제품 통합은 Security Hub CSPM으로 조사 결과를 전송하고 Security Hub CSPM으로부터 조사 결과를 수신할 수 있습니다.

Caveonix – Caveonix Cloud

통합 유형: 전송 및 수신

제품 ARN: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

Caveonix AI 기반 플랫폼은 클라우드 네이티브 서비스, VM 및 컨테이너를 다루면서 하이브리드 클라우드의 가시성, 평가 및 완화를 자동화합니다. AWS Security Hub CSPM과 통합되어 AWS 데이터와 고급 분석을 Caveonix 병합하여 보안 알림 및 규정 준수에 대한 인사이트를 제공합니다.

AWS Marketplace 링크

파트너 설명서

Cloud Custodian – Cloud Custodian

통합 유형: 전송 및 수신

제품 ARN: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian을(를) 사용하면 클라우드에서 사용자를 잘 관리할 수 있습니다. 간단한 YAML DSL을 통해 쉽게 정의된 규칙이 안전하고 최적화된 비용으로 관리성이 뛰어난 클라우드 인프라를 사용할 수 있도록 합니다.

제품 링크

파트너 설명서

DisruptOps, Inc. – DisruptOPS

통합 유형: 전송 및 수신

제품 ARN: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

DisruptOps 보안 작업 플랫폼은 조직이 자동화된 가드레일을 사용하여 클라우드에서 보안 모범 사례를 유지할 수 있도록 도와줍니다.

제품 링크

파트너 설명서

Kion

통합 유형: 전송 및 수신

제품 ARN: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion(이전 명칭 cloudtamer.io)는 AWS을(를) 위한 완벽한 클라우드 거버넌스 솔루션입니다. Kion은(는) 이해 관계자에게 클라우드 운영에 대한 가시성을 제공하고 클라우드 사용자가 계정을 관리하고, 예산 및 비용을 관리하고, 지속적인 규정 준수를 보장할 수 있도록 지원합니다.

제품 링크

파트너 설명서

Turbot – Turbot

통합 유형: 전송 및 수신

제품 ARN: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot은(는) 클라우드 인프라가 안전하고, 규정을 준수하며, 확장 가능하고, 비용에 최적화된 상태를 유지하도록 보장합니다.

제품 링크

파트너 설명서

## Security Hub CSPM과 사용자 지정 제품 통합

통합 AWS 서비스 및 타사 제품에서 생성된 조사 결과 외에도 AWS Security Hub CSPM은 다른 사용자 지정 보안 제품에서 생성된 조사 결과를 사용할 수 있습니다.

Security Hub CSPM API의 BatchImportFindings 작업을 사용하여 이러한 조사 결과를 Security Hub CSPM으로 전송할 수 있습니다. 동일한 작업을 사용하여 이미 Security Hub CSPM으로 전송한 사용자 지정 제품의 결과를 업데이트할 수 있습니다.

사용자 지정 통합을 설정할 때는 Security Hub CSPM 파트너 통합 가이드에 제공된 지침 및 체크리스트를 사용하세요.

## 사용자 지정 제품 통합에 대한 요구 사항 및 권장 사항

`BatchImportFindings` API 작업을 성공적으로 간접 호출하려면 Security Hub CSPM을 활성화해야 합니다.

또한 the section called “조사 결과 형식: ASFF”을(를) 사용하여 사용자 지정 제품에 대한 조사 결과 세부 정보를 제공해야 합니다. 사용자 지정 제품 통합에 대한 다음 요구 사항 및 권장 사항을 검토합니다.

제품 ARN 설정

Security Hub CSPM을 활성화하면 현재 계정에 Security Hub CSPM의 기본 제품 Amazon 리소스 이름(ARN)이 생성됩니다.

이 제품 ARN의 형식은 `arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default`입니다. 예제: `arn:aws:securityhub:us-west-2:123456789012:product/123456789012/default`.

`BatchImportFindings` API 작업을 간접적으로 호출할 때 이 제품 ARN을 `ProductArn` 속성 값으로 사용하세요.

회사 및 제품 이름 설정

조사 결과를 Security Hub CSPM으로 전송하는 사용자 지정 통합에 사용할 선호하는 회사 이름 및 제품 이름을 설정하는 데 `BatchImportFindings`를 사용할 수 있습니다.

지정된 이름은 각각 개인 이름 및 기본 이름이라고 하는 사전 구성된 회사 이름 및 제품 이름을 대체하며 Security Hub CSPM 콘솔 및 각 조사 결과의 JSON에 표시됩니다. 조사 결과 공급자에 대한 BatchImportFindings을(를) 참조하세요.

결과 ID 설정

`Id` 속성을 사용하여 자체 결과 ID를 공급하고, 관리하고, 증분해야 합니다.

각각의 새로운 조사 결과에는 고유한 결과 ID가 있어야 합니다. 사용자 지정 제품이 동일한 조사 결과 ID로 여러 조사 결과를 전송하는 경우, Security Hub CSPM은 첫 번째 조사 결과만 처리합니다.

계정 ID 설정

`AwsAccountId` 속성을 사용하여 자체 계정 ID를 지정해야 합니다.

생성 날짜 및 업데이트 날짜 설정

`CreatedAt` 및 `UpdatedAt` 속성에 자체 타임스탬프를 제공해야 합니다.

### 사용자 지정 제품의 조사 결과 업데이트

사용자 지정 제품에서 새로운 조사 결과를 전송할 뿐만 아니라 `BatchImportFindings` API 작업을 사용하여 사용자 지정 제품에서 기존 조사 결과를 업데이트할 수도 있습니다.

기존 조사 결과를 업데이트하려면 `Id` 속성을 통해 기존 조사 결과 ID를 사용합니다. 수정된 `UpdatedAt` 타임스탬프를 포함하여 요청에서 업데이트된 적절한 정보로 전체 결과를 다시 보냅니다.

### 사용자 지정 통합 예제

다음 예제 사용자 지정 제품 통합을 지침으로 사용하여 고유한 사용자 지정 솔루션을 생성할 수 있습니다.

Chef InSpec 스캔에서 Security Hub CSPM으로 조사 결과 전송

Chef InSpec 규정 준수 스캔을 실행한 다음 조사 결과를 Security Hub CSPM으로 전송하는 CloudFormation 템플릿을 생성할 수 있습니다.

자세한 내용은 Chef InSpec 및 AWS Security Hub CSPM을 사용한 지속적인 규정 준수 모니터링을 참조하세요.

Trivy에서 탐지한 컨테이너 취약성을 Security Hub CSPM으로 전송

를 사용하여 컨테이너의 취약성AquaSecurity Trivy을 스캔한 다음 해당 취약성 조사 결과를 Security Hub CSPM으로 전송하는 CloudFormation 템플릿을 생성할 수 있습니다.

자세한 내용은 Trivy 및AWS Security Hub CSPM을 사용하여 컨테이너 취약성 스캔을 위한 CI/CD 파이프라인을 구축하는 방법을 참조하세요.

## Security Hub CSPM과 Microsoft Azure 통합

Microsoft Azure 리소스를 모니터링하기 위해 Microsoft Azure를 AWS Security Hub CSPM과 통합할 수 있습니다. 그러면 Security Hub CSPM이 Azure 환경에 대한 태세 관리 검사를 자동으로 활성화하고 환경에 대한 조사 결과를 생성합니다. 보다 구체적으로, 서비스는 다음을 제공합니다.

> **Note**
>
> Security Hub CSPM 콘솔, APIs 및를 사용하여 Azure 표준 및 제어를 관리할 수 있습니다 AWS CloudFormation. Security Hub CSPM 중앙 구성 기능은 Azure 표준에서 지원되지 않습니다.

- ASFF 조사 결과 - Security Hub CSPM은 Azure 리소스에 대해 수행하는 태세 확인을 위해 AWS Security Finding Format(ASFF) 형식으로 조사 결과를 생성합니다.
- CIS Microsoft Azure Foundations Benchmark v4.0 - CIS Azure v4.0 표준에 대한 자동화된 규정 준수 검사. 이 표준에는 자격 증명, 네트워킹, 스토리지, 로깅 및 데이터베이스 제어가 포함됩니다.
- Azure 기본 모범 사례 AWS- 네트워크 보안, 자격 증명 관리, 데이터 보호 및 로깅을 다루는 선별된 보안 모범 사례를 기반으로 Azure 리소스 구성 오류를 자동으로 감지합니다.
- 태세 관리 - 보안 모범 사례 및 규정 준수 표준을 기준으로 Azure 리소스 구성을 지속적으로 평가하며, 두 표준에 걸쳐 122개의 제어를 제공합니다.
- 공급자별 보안 점수 - 각 환경을 독립적으로 추적할 수 있도록 AWS 및 Azure의 보안 점수를 구분합니다.

통합을 생성하려면 다음 프로세스를 통해 Azure 환경을 Security Hub CSPM에 연결합니다.

> **Note**
>
> Azure 표준은 다음과 같은 점에서 AWS 표준과 다릅니다.
>
> - Azure 표준에는 수동 AWS Config 사전 조건이 필요하지 않습니다. CSPM 전용 고객에게 고객 관리형 레코더가 필요한 AWS경우와 달리 Azure 표준은 내부 서비스 연결 레코더를 자동으로 사용합니다.
> - Azure 표준은 항상 내부 서비스 연결 구성 규칙을 사용합니다. AWS 표준은 Security Hub도 활성화된 경우에만 서비스 연결 구성 규칙을 사용합니다.

1. 애플리케이션 등록, 페더레이션 자격 증명, Azure 역할 할당 및 Event Hub 인프라를 사용하여 Azure 환경을 구성합니다.
2. Security Hub CSPM 콘솔을 사용하여 통합을 위한 커넥터를 생성합니다. Azure 테넌트 ID, 애플리케이션 클라이언트 ID 및 모니터링 범위를 지정합니다.
3. AWS Config 는 Azure 환경에서 리소스 구성 데이터를 수집합니다.

   AWS Config 는 내부적으로 리소스 구성 데이터를 수집하는 데 사용됩니다. 기록을 명시적으로 활성화 AWS Config 하고 비용을 지불해야 하는 태세 관리와 달리 AWS Azure 태세 관리는 AWS Config 자동으로 처리합니다. 별도로 활성화 AWS Config 하거나, 레코더를 구성하거나, AWS Config 사용량에 대해 별도로 지불할 필요가 없습니다. 이러한 비용은 Security Hub CSPM 요금에 포함됩니다.
4. Security Hub CSPM은 Azure 환경에서 리소스 구성 데이터 및 활동 로그 이벤트를 수신하기 시작합니다.

5. Security Hub CSPM은 Azure 환경에 대한 태세 관리 조사 결과를 생성합니다.

## AWS Config 를 사용하는 방법

AWS Config 는 내부적으로 리소스 구성 데이터를 수집하고 Azure 환경의 변경 사항을 감지하는 데 사용됩니다. 커넥터는 이를 자동으로 처리합니다. AWS Config 별도로 활성화하거나, 레코더를 구성하거나, AWS Config 사용량을 지불할 필요가 없습니다. 이러한 비용은 Azure 리소스에 대한 Security Hub CSPM 요금에 포함됩니다.

## 서비스 연결 커넥터 및 고객 관리형 커넥터

Security Hub CSPM은 두 가지 유형의 커넥터를 지원합니다.

서비스 연결 커넥터(SLC)

Security Hub에서 Azure 통합을 설정할 때 자동으로 생성됩니다. 서비스 연결 커넥터의 범위는 항상 Security Hub 커넥터에 정의된 범위와 일치합니다. 서비스 연결 커넥터의 범위는 직접 수정할 수 없으며 대신 Security Hub에서 범위를 수정합니다. Security Hub는 사용자를 대신하여 서비스 연결 커넥터의 수명 주기를 관리합니다.

고객 관리형 커넥터(CMC)

통합 페이지의 Security Hub CSPM 콘솔에서 직접 생성됩니다. Security Hub와 독립적으로 Security Hub CSPM을 사용하려는 경우 또는 Security Hub 커넥터와 다른 범위가 필요한 경우 고객 관리형 커넥터를 사용합니다. 두 유형이 모두 있는 경우 서비스 연결 커넥터 범위는 항상 고객 관리형 커넥터 범위보다 크거나 같아야 합니다.

> **Note**
>
> Security Hub와 달리 Security Hub CSPM은 Azure 커넥터에 대한 기능별 선택을 제공하지 않습니다. Security Hub CSPM에서 커넥터를 생성하면 모든 태세 관리 기능이 함께 활성화됩니다.

Security Hub CSPM을 Azure와 통합하기 위한 비용 예측 및 계산에 대한 자세한 내용은 AWS Security Hub CSPM 요금을 참조하세요.

주제

- Security Hub CSPM을 Microsoft Azure와 통합하기 위한 사전 조건
- Security Hub CSPM과 통합되도록 Microsoft Azure 구성
- Security Hub CSPM을 Microsoft Azure와 통합하도록 구성
- Security Hub CSPM에서 Microsoft Azure 커넥터 삭제


# Security Hub CSPM을 Microsoft Azure와 통합하기 위한 사전 조건

Microsoft Azure를 AWS Security Hub CSPM과 통합하기 전에 및 Azure 환경에서 다음 작업을 AWS 완료합니다. 이렇게 하면 사용자와 Security Hub CSPM이 Azure 리소스를 모니터링하는 데 필요한 리소스와 권한을 갖게 됩니다.

주제


- 에 대한 사전 조건 AWS
- Microsoft Azure의 사전 조건


## 에 대한 사전 조건 AWS

에 AWS 계정다음이 있는지 확인합니다.

AWS Security Hub CSPM 활성화

Security Hub CSPM은 커넥터를 생성할 AWS 계정 및 AWS 리전 에서 활성화해야 합니다.

콘솔 IAM 권한

커넥터를 생성하는 IAM 보안 주체에는 다음 권한이 있어야 합니다.

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

IAM 아웃바운드 자격 증명 연동 활성화됨

에서 IAM 아웃바운드 자격 증명 연동을 활성화해야 합니다 AWS 계정. 이 기능을 사용하면 AWS 서비스가 수명이 긴 보안 암호가 아닌 페더레이션 자격 증명을 사용하여 외부 자격 증명 공급자(예: Microsoft Entra ID)에 인증할 수 있습니다.

아웃바운드 자격 증명 연동을 활성화한 후 토큰 발급자 URL을 기록해 둡니다. 이 URL은 형식을 따릅니다.

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

Azure에서 페더레이션 ID 자격 증명을 구성할 때이 URL이 필요합니다.

## Microsoft Azure의 사전 조건

Azure 환경에 다음이 있는지 확인합니다.

Azure 테넌트

Azure 상용 클라우드에 Azure 테넌트가 있어야 합니다. Azure Government 및 Azure China는 지원되지 않습니다.

Microsoft Entra ID 로그 가용성

리소스 기록에는 Microsoft Entra ID 테넌트의 Microsoft Graph 감사 로그 및 로그인 로그가 필요합니다. 일부 Microsoft Entra ID 로그에는 Microsoft Entra ID P1 또는 P2 라이선스가 필요합니다.

테넌트에 필요한 로그가 없는 경우 리소스 기록에서 부분적인 실패를 보고할 수 있습니다. 앱 등록 및 Azure 역할 할당은 누락된 로그 데이터를 제공하지 않습니다.

글로벌 관리자 역할

Azure 환경을 구성하는 사람은 Microsoft Entra ID에 글로벌 관리자 역할이 있어야 합니다. 이 역할은 애플리케이션을 등록하고, Microsoft Graph API 권한에 대한 관리자 동의를 부여하고, 테넌트 루트 관리 그룹 범위에서 RBAC 역할을 할당하고, Entra ID 감사 로그에 대한 진단 설정을 구성하는 데 필요합니다.

> **Note**
>
> 많은 조직에서 Azure 글로벌 관리자와 AWS 보안 관리자는 서로 다른 사람입니다. Azure 설정은 생성된 설정 스크립트를 사용하여 독립적으로 완료할 수 있습니다.

Azure 앱 등록

Microsoft Entra ID로 애플리케이션을 등록해야 합니다. 이 애플리케이션은가 연합 자격 증명을 사용하여 Azure 환경에 인증하는 데 AWS 사용하는 자격 증명 역할을 합니다. 클라이언트 보안 암호는 필요하지 않습니다.

Azure Event Hub

활동 로그 및 Entra ID 감사 로그 이벤트를 수신하려면 Azure Event Hub 네임스페이스 및 Event Hub 인스턴스를 생성해야 합니다. 설정 스크립트는이 생성을 자동화합니다.

Microsoft Graph API 권한

등록된 애플리케이션에는 다음과 같은 Microsoft Graph API 권한이 필요합니다(애플리케이션 유형, 관리자 동의 필요).

- `Directory.Read.All` - 사용자, 그룹 및 서비스 보안 주체를 포함한 디렉터리 데이터를 읽습니다.
- `AuditLog.Read.All` - Entra ID 감사 로그 이벤트를 읽습니다.
- `Policy.Read.All` - 조직 정책 및 조건부 액세스 구성을 읽습니다.

Azure RBAC Reader 역할

서비스 보안 주체는 테넌트 루트 관리 그룹 범위에서 리더 역할을 할당받아야 합니다. 이렇게 하면 테넌트의 모든 구독에서 모든 Azure 리소스에 대한 읽기 전용 액세스 권한이 부여됩니다.

이러한 작업을 완료하면 Azure 환경을 구성할 준비가 된 것입니다.

## Security Hub CSPM과 통합되도록 Microsoft Azure 구성

사전 필수 작업을 완료한 후 AWS Security Hub CSPM과의 통합을 지원하도록 Microsoft Azure 환경을 구성할 수 있습니다. 이를 위해 Security Hub CSPM 콘솔은 구성에 맞게 사용자 지정된 설정 스크립트를 생성합니다.

스크립트를 생성하려면 다음을 수행합니다.

1. Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 통합을 선택합니다.
3. Azure 커넥터 생성을 선택합니다.
4. 커넥터 구성(테넌트 ID, 범위 및 이름)을 완료한 다음 생성된 설정 스크립트를 복사합니다.

스크립트를 실행하려면 Azure CLI를 사용하고 글로벌 관리자 계정()으로 인증합니다`az login`.

스크립트를 실행하면 일련의 작업이 수행됩니다. 다음 섹션에서는 스크립트가 수행하는 각 작업에 대해 설명합니다. 조직에서 스크립트 실행을 제한하는 경우이 주제를 지침으로 사용하여 이러한 작업을

수동으로 수행할 수 있습니다. Azure 환경을 구성한 후 Azure와 통합하도록 Security Hub CSPM을 구성할 수 있습니다.

> **Note**
>
> 단일 Azure 앱 등록은 AWS 보안 서비스 간에 공유됩니다. 또한 Security Hub 또는 Azure용 Amazon Inspector를 사용하는 경우 동일한 앱 등록을 사용합니다. 각 AWS 서비스에 대해 별도의 등록을 생성할 필요는 없습니다.

작업

- 1단계: Azure 애플리케이션 등록
- 2단계: 서비스 보안 주체 생성
- 3단계: 페더레이션 자격 증명 구성
- 4단계: 리더 역할 할당
- 5단계: Microsoft Graph API 권한 구성
- 6단계: Azure Event Hub 설정
- 7단계: 활동 로그 및 Entra ID 감사 로그 내보내기 구성

## 1단계: Azure 애플리케이션 등록

Microsoft Entra ID에 새 애플리케이션을 등록합니다. 이 애플리케이션은가 연합 자격 증명을 사용하여 Azure 환경에 인증하는 데 AWS 사용하는 자격 증명 역할을 합니다. 클라이언트 보안 암호는 필요하지 않습니다.

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

출력의 애플리케이션(클라이언트) ID(appId속성)를 기록해 둡니다. Security Hub CSPM 콘솔에서 커넥터를 생성할 때이 값을 제공합니다.

## 2단계: 서비스 보안 주체 생성

등록된 애플리케이션에 대한 서비스 보안 주체를 생성합니다. Azure 역할 할당을 사용하여 서비스 보안 주체에 권한을 부여합니다. 서비스 보안 주체는 Azure 환경에서 작업을 수행합니다.

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

여기서 *application-client-id*는 이전 단계의 애플리케이션(클라이언트) ID입니다.

### 3단계: 페더레이션 자격 증명 구성

가 클라이언트 보안 암호 없이 인증할 AWS 수 있도록 애플리케이션에서 페더레이션 자격 증명을 구성합니다. 이렇게 하면 AWS 와 Azure 간에 OIDC 신뢰가 설정됩니다. 수명이 긴 보안 암호 또는 자격 증명은 저장되지 않습니다.

```
$ 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"
  }'
```

키 값:

- 발급자 - IAM 아웃바운드 자격 증명 연동의 토큰 발급자 URL입니다. 형식에 따릅니다`https://uuid.tokens.sts.global.api.aws`.
- 제목 -에서 `AWSServiceRoleForConfigThirdParty` 서비스 연결 역할의 ARN입니다 AWS 계정.는 커넥터 설정 중에이 서비스 연결 역할을 자동으로 AWS 생성합니다.
- 대상 - `api://AzureADTokenExchange` (워크로드 ID 페더레이션의 표준 값).

### 4단계: 리더 역할 할당

루트 범위()에서 서비스 보안 주체에 리더 역할을 할당합니다`/`. 이렇게 하면 테넌트의 모든 구독에서 모든 Azure 리소스에 대한 읽기 전용 액세스 권한이 부여됩니다.

> **⚠ 루트 범위에서 리더 할당**
>
> 테넌트 루트 관리 그룹 범위가 아닌 루트 범위(`/`)에서 리더 역할을 할당해야 합니다. Security Hub CSPM은 테넌트 루트에 범위가 지정된 할당을 포함하여 모든 범위에서 Azure 역할 할당 리소스를 읽습니다. 루트 관리 그룹의 리더 할당은 범위가 인 할당을 다루지 않으므로 `/`읽기가 실패하고 권한 부여 오류가 발생하며 커넥터가 성능 저하 상태가 될 수 있습니다.

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

**루트 범위 할당에는 승격된 액세스가 필요합니다.**

루트 범위(/)에서 역할을 할당하려면 승격된 액세스 권한이 필요합니다. 역할 할당에 실패하면 Microsoft Entra ID > 속성에서 Azure 리소스에 대한 액세스 관리가 예로 설정되어 있는지 확인합니다. 그런 다음 로그아웃했다가 다시 로그인하여 토큰을 새로 고칩니다.

**임시 루트 고도 제거**

Azure 리소스에 대한 액세스 관리를 활성화하면 로그인한 관리자에게 루트 범위(/)의 사용자 액세스 관리자 역할이 부여되며,이 역할은 테넌트의 모든 구독 및 관리 그룹에서 액세스를 관리할 수 있습니다. 온보딩이 완료되면 Azure 리소스에 대한 액세스 관리를 Microsoft Entra ID > 속성에서 아니요로 다시 설정하여이 고도가 활성 상태로 유지되지 않도록 합니다.

### 5단계: Microsoft Graph API 권한 구성

애플리케이션에 다음 Microsoft Graph API 권한(애플리케이션 유형)을 부여한 다음 관리자 동의를 부여합니다.

- `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
```

## 6단계: Azure Event Hub 설정

AWS Config 는 Azure Event Hub를 사용하여 Azure 환경의 리소스 구성 변경 사항에 대한 알림을 거의 실시간으로 수신합니다. 설정 스크립트는 Event Hub 인프라를 생성하고 검색을 위해 태그를 지정합니다.

```
$ 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"
```

Event Hub를 생성한 후 검색할 네임스페이스에 태그를 지정하고 데이터 수신자 역할을 할당합니다.

```
$ 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**
>
> 태그 형식에서 `AWSConfig-`*`account-id`*`-`*`region`* *`account-id`*는 12자리 AWS 계정 ID이고 *`region`*은 커넥터를 생성하는 AWS 리전 입니다(예: `us-east-1`). 이러한 값은이 Event Hub 통합을 소유한 AWS 계정 및 리전을 식별합니다.

주요 구성:

- 네임스페이스 SKU - 표준(소비자 그룹에 필요).
- Event Hub 이름 - `activitylog`.
- 소비자 그룹 - `AWSConfig`.
- 태그 - `AWSConfig-`*`account-id`*`-`*`region`* 값이 있는 입니다`activitylog`. 이 태그를 사용하면 AWS Config 가 Event Hub를 자동으로 검색할 수 있습니다.
- 역할 할당 - 네임스페이스의 Azure Event Hubs 데이터 수신기입니다.

## 7단계: 활동 로그 및 Entra ID 감사 로그 내보내기 구성

활동 로그 및 Entra ID 감사 로그를 Event Hub로 내보내도록 Azure를 구성합니다.

활동 로그 내보내기:

각 구독에 대한 진단 설정을 구성하여 활동 로그를 Event Hub로 내보냅니다. 설정 스크립트는 모니터링되는 모든 구독에 대해 이를 자동으로 구성합니다. 활동 로그는 역할 할당 및 리소스 변경을 포함한 구독 수준 활동을 캡처합니다.

Entra ID 감사 로그 내보내기:

감사 로그를 동일한 Event Hub로 내보내도록 Microsoft Entra ID에서 진단 설정을 구성합니다. Microsoft Entra ID > 모니터링 > 진단 설정 > 진단 설정 추가로 이동합니다. AuditLogs를 활성화하고 Event Hub로 라우팅합니다.

Microsoft Defender for Cloud 연속 내보내기(선택 사항):

Cloud용 Defender 보안 알림을 Security Hub CSPM에 전달하려면 Event Hub로 연속 내보내기를 구성합니다. Azure 포털에서 Microsoft Defender for Cloud > 환경 설정 > 구독 선택 > 연속 내보내기로 이동합니다. Event Hub를 내보내기 대상으로 선택하고 Event Hub 네임스페이스를 선택합니다. 보안 알림을 내보내기 데이터 유형으로 활성화합니다.

Amazon Inspector 데이터 이벤트 구성(선택 사항):

Azure VM 스캔에 Amazon Inspector를 사용하려는 경우 추가 데이터 이벤트 구성이 필요합니다. Inspector별 데이터 이벤트 구성에 대한 자세한 내용은 Azure 통합을 위한 Amazon Inspector 설명서를 참조하세요.

## Security Hub CSPM을 Microsoft Azure와 통합하도록 구성

사전 필수 작업을 완료하고 Microsoft Azure 환경을 구성한 후 Azure와 통합하도록 AWS Security Hub CSPM을 구성할 수 있습니다. Azure와 통합되도록 Security Hub CSPM을 구성하려면 커넥터를 생성합니다. 커넥터를 생성한 후 다음 이벤트가 발생합니다.

1. Security Hub CSPM은 Azure 자격 증명과 Azure 환경에 대한 연결을 검증합니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다.
2. AWS Config 는 Azure 리소스에 대한 구성 데이터를 검색하고 기록하기 시작합니다.
3. Security Hub CSPM은 리소스 데이터 수집이 완료된 후 Azure 리소스에 대한 태세 관리 조사 결과를 생성하기 시작합니다.

> **Note**
>
> Security Hub에서 커넥터를 이미 생성한 경우 Security Hub CSPM에서 서비스 연결 커넥터가 자동으로 생성됩니다. 다른 범위가 필요하지 않은 한 별도의 고객 관리형 커넥터를 생성할 필요가 없습니다.

주제

- Azure 커넥터 생성
- 표준 및 제어 활성화
- Azure 커넥터의 범위 조정
- Azure 커넥터의 상태 확인
- Azure 커넥터 문제 해결

- Security Hub CSPM이 리소스 식별자를 처리하는 방법
- Azure에 사용 가능한 제어

## Azure 커넥터 생성

환경에 맞는 Microsoft Azure 커넥터를 생성하려면 AWS Security Hub CSPM 콘솔 또는 API를 사용하여 다음 단계를 완료합니다.

1. Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 통합을 선택합니다.
3. Azure 커넥터 생성을 선택합니다.
4. Azure 테넌트 ID에 Azure Active Directory 테넌트 식별자를 입력합니다.
5. 애플리케이션(클라이언트 ID)에 생성한 Azure 앱 등록의 애플리케이션 ID를 입력합니다.
6. 다음을 수행하여 추가 설정과 커넥터 범위를 구성합니다.

   - 이름에 커넥터의 고유한 이름을 입력합니다. 이름은 최대 50자의 영숫자를 포함할 수 있으며 하이픈(-)을 포함할 수 있습니다.

     > **Important**
     >
     > 이름과 설명은 콘텐츠를 식별하는 데 사용되며 민감한 정보, 기밀 정보 또는 개인 식별 정보(PII)를 포함하지 않는 것이 좋습니다.

   - 설명에 필요에 따라 커넥터에 대한 간략한 설명을 입력합니다. 설명은 최대 200자를 포함할 수 있습니다.
   - 구독의 경우 모든 구독을 선택하여 테넌트의 모든 현재 및 미래 구독을 모니터링하거나 특정 구독을 선택하여 지정한 구독만 모니터링합니다. 특정 구독만 모니터링하도록 선택한 경우 각 구독의 ID를 입력합니다.
   - 리전에서 리소스가 배포되는 Azure 리전을 선택합니다.

     > **Note**
     >
     > Microsoft Entra ID 및 Microsoft Graph 리소스를 평가하는 컨트롤을 사용하려면 통합 구성에 글로벌 리전 범위를 포함해야 합니다. 특정 Azure 리전만 선택하면 이러한 제어는 결과를 생성하지 않습니다.

7. 구성을 검토하고 커넥터 생성을 선택합니다.

커넥터를 생성한 후 Security Hub CSPM은 Azure 자격 증명을 검증하고 리소스 검색을 시작합니다. 커넥터는 2~5분 이내에 활성 상태를 표시해야 합니다.

## 표준 및 제어 활성화

커넥터를 생성한 후 Azure 보안 표준을 활성화하여 결과 생성을 시작해야 합니다. 표준 활성화 및 제어 관리에 대한 일반적인 내용은 표준 활성화 및 제어 활성화 및 비활성화를 참조하세요.

사용 가능한 표준

- CIS Microsoft Azure Foundations Benchmark v4.0 - Azure 환경 보안을 위한 모범 사례를 정의하는 널리 채택된 보안 벤치마크입니다. 각 제어는 Azure 구성의 특정 측면(예: 스토리지 계정 암호화, 네트워크 보안 그룹 규칙, 자격 증명 및 액세스 설정)을 평가합니다.
- Azure 기본 모범 사례 - 네트워크 연결성, 퍼블릭 액세스 및 민감한 데이터 지표를 상호 연관시켜 Azure 리소스의 노출 위험을 평가합니다. 위험이 높은 리소스를 강조하는 노출 유형 조사 결과를 생성합니다.

Azure 표준에는 컨트롤과 별도로 자체 AWS 컨트롤 세트가 있습니다. 단일 검사로 AWS 및 Azure 리소스를 모두 평가하는 교차 클라우드 제어는 없습니다.

표준 활성화

Security Hub CSPM 콘솔 또는 API/CLI를 통해 Azure 표준을 활성화할 수 있습니다. Security Hub CSPM 콘솔에서 표준으로 이동하여 원하는 표준을 활성화합니다. 또는 CLI를 사용합니다.

```
$ aws securityhub batch-enable-standards \
  --standards-subscription-requests '[{"StandardsArn": "Standard-ARN"}]' \
  --region your-aws-region
```

> **Note**
>
> 커넥터를 생성하기 전이나 후에 Azure 표준을 활성화할 수 있습니다. 커넥터는 결합되지 않습니다. 그러나 조사 결과는 커넥터와 표준이 모두 활성 상태이고 리소스 데이터가 수집된 후에만 생성됩니다.

개별 컨트롤 관리

표준이 활성화되면(일반적으로 몇 초 이내) 개별 컨트롤을 보고 관리할 수 있습니다.

- 컨트롤 보기: Security Hub CSPM 콘솔(표준 > 표준 선택 > 컨트롤) 또는 `list-standards-control-associations` API를 사용합니다.
- 컨트롤 비활성화: 환경에 특정 컨트롤을 적용할 수 없는 경우 해당 컨트롤을 비활성화할 수 있습니다.
- 사용자 지정 파라미터 구성: 일부 컨트롤은 사용자 지정 입력 파라미터(예: 암호 길이 임계값)를 허용합니다. API를 통해 구성할 수 있습니다`update-security-control`.

중요 정보

- Azure 표준은 전체 커넥터 범위에 균일하게 적용됩니다. 동일한 커넥터 내에서 다른 Azure 구독에 대해 다른 표준 또는 제어를 활성화할 수 없습니다.
- 제어는 리소스 데이터 가용성에 따라 달라집니다. 각 컨트롤은 특정 Azure 리소스 유형을 평가합니다. AWS Config 가 특정 리소스 유형에 대한 구성 데이터를 아직 수집하지 않은 경우 제어는 해당 리소스에 대한 기본 PASS 결과를 생성합니다. 이러한 기본 PASS 조사 결과는 리소스 데이터가 도착하면 정확한 평가로 자동 업데이트됩니다. 리소스 데이터 수집이 완료될 때까지 초기 규정 준수 점수를 정확한 것으로 취급하지 마십시오.
- 커넥터를 생성하기 전에도 보안 제어를 위한 사용자 지정 입력 파라미터를 구성할 수 있습니다. 이러한 파라미터는 독립적으로 유지됩니다.
- 구독 수준 설정(예: Microsoft Defender 플랜, 활동 로그 알림)을 평가하는 제어는 개별 리소스가 아닌 Azure 구독당 하나의 결과를 생성합니다.
- 멀티클라우드 표준은 중앙 구성 정책에 포함될 수 없습니다. 각 AWS 계정 및에서 Azure 표준 활성화를 독립적으로 관리해야 합니다 AWS 리전.

## Azure 커넥터의 범위 조정

Microsoft Azure 커넥터를 생성한 후 모니터링하는 Azure 구독 또는 Azure 리전을 변경하여 커넥터의 범위를 조정할 수 있습니다. 범위를 조정하면 대부분의 변경 유형이 약 15분 이내에 적용됩니다.

범위를 조정하기 전에 다음 사항에 유의하세요.

- 고객 관리형 커넥터의 범위는 동일한 계정 및 리전에 있는 기존 서비스 연결 커넥터의 범위를 초과할 수 없습니다.

- 범위를 확장하면 Security Hub CSPM은가 구성 데이터를 AWS Config 수집한 후 새 리소스에 대한 조사 결과를 생성하기 시작합니다.
- 범위를 줄이면 제거된 리소스에 대한 기존 결과가 아카이브된 상태로 전환됩니다.

## Azure 커넥터의 상태 확인

언제든지 Microsoft Azure 커넥터의 상태를 확인할 수 있습니다. Security Hub CSPM 콘솔에서 통합으로 이동하여 커넥터에 활성 상태가 표시되는지 확인합니다.

초기 결과는 일반적으로 리소스 데이터 수집이 완료된 후 15~30분 이내에 나타납니다.

> **Note**
>
> 커넥터 상태는 최종적으로 일관됩니다. 권한 또는 구성 문제가 발생하면 커넥터 상태가 실행 가능한 메시지와 함께 빠르게 성능 저하로 변경됩니다. 그러나 문제를 해결한 후 상태가 연결됨으로 돌아가는 데 최대 24시간이 걸릴 수 있습니다.
>
> - 최근 수정 후 성능 저하 상태가 반드시 지속적인 문제를 나타내는 것은 아닙니다.
> - 기록 실패에 대한 실시간 가시성을 얻으려면 네임스페이스에서 CloudWatch 지표를 확인하세요.

## Azure 커넥터 문제 해결

커넥터에 문제가 발생하면 다음 정보를 사용하여 일반적인 문제를 진단하고 해결합니다.

커넥터 상태가 비정상임

이 문제는 일반적으로 Azure에서 페더레이션 자격 증명이 올바르게 구성되지 않은 경우에 발생합니다.

이 문제를 해결하려면 Azure 페더레이션 자격 증명의 토큰 발급자 URL 및 주체 ARN이와 일치하는지 확인합니다 AWS 계정.

30분 후 결과 없음

이 문제는 Event Hub가 활동 로그를 수신하지 않거나 활성화된 표준이 없는 경우에 발생할 수 있습니다.

이 문제를 해결하려면 Event Hub 네임스페이스에 태그를 올바르게 지정하고 (`AWSConfig-account-id-region=activitylog`), `AWSConfig` 소비자 그룹이 존재하고, 데이터 수신자 역할이 할당되고, 하나 이상의 Azure 표준이 활성화되어 있는지 확인합니다.

일부 Azure 리소스를 기록할 수 없음

오류는 다음과 같은 이유로 발생할 수 있습니다.

- Azure 환경이 리소스 기록의 사전 조건을 충족하지 않습니다.
- 앱 등록에는 Microsoft Graph API 권한에 대한 관리자 동의가 없습니다.
- 리더 역할 할당에 필요한 모든 범위가 포함되지는 않습니다.
- Microsoft Entra ID 테넌트에 필요한 로그 데이터가 없습니다.

오류를 해결하려면 다음을 수행합니다.

1. 환경이 모든 요구 사항을 충족하는지 확인하려면 Microsoft Azure의 사전 조건을 검토하세요.
2. 앱 등록에 관리자의 동의를 받아 필요한 Microsoft Graph API 권한이 있는지 확인합니다.
3. 서비스 보안 주체가 테넌트 루트 관리 그룹 범위에 리더 역할을 가지고 있는지 확인합니다.

커넥터가 보류 중 상태로 유지됨

Azure 앱 등록이 잘못 구성된 경우이 문제가 발생할 수 있습니다.

이 문제를 해결하려면 페더레이션 자격 증명 발급자 URL과 주제 식별자가와 일치하는지 확인합니다 AWS 계정. 또한 필요한 모든 Microsoft Graph API 권한에 대해 관리자 동의가 부여되었는지 확인합니다.

## Security Hub CSPM이 리소스 식별자를 처리하는 방법

AWS Security Hub CSPM용 Azure 통합을 활성화하면 다른 클라우드 공급자의 리소스 식별자가 다른 클라우드 공급자로부터 수집된 해당 리소스 구성 데이터의 관리와 관련된 메타데이터로 AWS Config AWS Security Hub CSPM 및 기타 AWS 서비스(필요한 경우)에 저장됩니다. 이러한 리소스 식별자는 사용자의 콘텐츠를 구성하지 않으므로 민감한 정보, 기밀 정보 또는 개인 식별 정보를 포함하지 않는 것이 좋습니다.

연결된 클라우드 환경의 다음 식별자는에서 멀티클라우드 보안 기능을 제공하기 AWS 위해 저장되고 사용됩니다.

- 리소스 식별자: Azure 테넌트 ID, 구독 ID, 위치(리전), 리소스 ID(리소IDs 또는 이름, 리소스 공급자, 리소스 유형)

리소스가 서로 어떤 관련이 있는지, 조사 결과가 리소스와 어떤 관련이 있는지를 포함하여 이러한 식별자 간의 관계는 서비스 메타데이터로도 저장됩니다.는 조사 결과를 리소스, 서비스 운영 로깅 및 중복 제거에 연결하여 리소스 상관 관계를 위해 이러한 식별자를 AWS 사용합니다.

## Azure에 사용 가능한 제어

Azure 표준을 활성화하면 다음 122 제어가 Azure 리소스를 평가합니다. 제어는 다음 두 가지 표준에 분산됩니다.

- CIS Microsoft Azure Foundations Benchmark v4.0 – 특정 CIS 섹션에 매핑된 96개의 제어
- Azure 기본 모범 사례 - 추가 보안 모범 사례를 다루는 26가지 제어

> **Note**
>
> Microsoft Entra ID 및 Microsoft Graph 리소스를 평가하는 컨트롤을 사용하려면 통합 구성에 글로벌 리전 범위를 포함해야 합니다.

사용 가능한 Azure 제어

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| 관리형 자격 증명이 활성화된 Azure 컨테이너 앱은 최소 권한을 따라야 합니다. | `microsoft.app/containerapps` | Azure 기본 모범 사례 |
| Azure Container Apps는 Azure SDK 자격 증명을 환경 변수로 전달해서는 안 됩니다. | `microsoft.app/containerapps` | Azure 기본 모범 사례 |
| Azure Container Apps에는 외부 수신이 활성화되어 있지 않아야 합니다. | `microsoft.app/containerapps` | Azure 기본 모범 사례 |
| Azure 컨테이너 앱 환경에는 무제한 NSG 액세스 권한이 없어야 합니다. | `microsoft.app/containerapps` | Azure 기본 모범 사례 |
| Azure Container App 관리형 환경에는 퍼블릭 IP가 활성화되어 있지 않아야 합니다. | `microsoft.app/managedenvironments` | Azure 기본 모범 사례 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure 역할 할당은 구독 범위에서 광범위한 관리자 액세스 권한을 부여해서는 안 됩니다. | `microsoft.authorization/roleassignments` | Azure 기본 모범 사례 |
| Azure 역할 할당은 사용자 액세스 관리자 역할을 부여해서는 안 됩니다. | `microsoft.authorization/roleassignments` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 사용자 지정 역할 정의에는 와일드카드 관리 권한이 없어야 합니다. | `microsoft.authorization/roledefinitions` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft 클라우드 보안 벤치마크 정책 할당에는 적용 모드가 활성화되어 있어야 합니다. | `microsoft.authorization/policyassignments` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Kubernetes Service(AKS) 클러스터에는 IP 제한 없이 공개적으로 액세스할 수 있는 API 서버가 없어야 합니다. | `microsoft.containerservice/managedclusters` | Azure 기본 모범 사례 |
| Azure Kubernetes Service(AKS) 클러스터는 유휴 시 Kubernetes 보안 암호를 암호화해야 합니다. | `microsoft.containerservice/managedclusters` | Azure 기본 모범 사례 |
| Azure Kubernetes Service(AKS) 클러스터는 지원되는 Kubernetes 버전을 실행해야 합니다. | `microsoft.containerservice/managedclusters` | Azure 기본 모범 사례 |
| Azure Cosmos DB 계정에는 연속 백업이 활성화되어 있어야 합니다. | `microsoft.documentdb/databaseaccounts` | Azure 기본 모범 사례 |
| Azure Database for MySQL 유연한 서버에는 퍼블릭 네트워크 액세스가 비활성화되어 있어야 합니다. | `microsoft.dbformysql/flexibleservers` | Azure 기본 모범 사례 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure Databricks 워크스페이스는 고객 관리형 가상 네트워크에 배포해야 합니다. | `microsoft.databricks/workspaces` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Databricks 워크스페이스에는 진단 로그 전송이 구성되어 있어야 합니다. | `microsoft.databricks/workspaces` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Databricks 워크스페이스는 관리형 디스크 암호화에 고객 관리형 키를 사용해야 합니다. | `microsoft.databricks/workspaces` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra ID 권한 부여 정책은 기본 사용자가 애플리케이션을 등록하는 것을 금지해야 합니다. | `microsoft.graph/policies/authorizationpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Entra ID에는 보안 기본값이 활성화되어 있어야 합니다. | `microsoft.graph/policies/identitysecuritydefaultsenforcementpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra 테넌트에는 허용되지 않는 지리적 위치에서의 액세스를 차단하는 조건부 액세스 정책이 있어야 합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra 테넌트에는 디바이스 코드 인증 흐름을 차단하는 조건부 액세스 정책이 있어야 합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 조건부 액세스 정책에는 모든 사용자에게 MFA가 필요합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra 테넌트는 조건부 액세스 정책을 통해 위험한 로그인을 위해 멀티 팩터 인증을 요구해야 합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure 테넌트는 Azure Service Management API에 대한 조건부 액세스를 통해 MFA가 필요합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| 하나 이상의 조건부 액세스 정책에는 Microsoft 관리 포털용 MFA가 필요합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra 권한 부여 정책은 관리자가 아닌 사용자가 테넌트를 생성하지 못하도록 제한해야 합니다. | `microsoft.graph/policies/authorizationpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra ID 인증 방법 정책은 재확인 기간을 0이 아닌 값으로 설정해야 합니다. | `microsoft.graph/policies/authenticationmethodspolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra 권한 부여 정책은 애플리케이션에 대한 사용자 동의를 제한해야 합니다. | `microsoft.graph/policies/authorizationpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 권한 부여 정책은 확인된 게시자 앱에 대한 사용자 동의를 제한해야 합니다. | `microsoft.graph/policies/authorizationpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra 권한 부여 정책은 게스트 사용자 액세스를 자신의 디렉터리 객체로 제한해야 합니다. | `microsoft.graph/policies/authorizationpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 권한 부여 정책은 게스트 초대를 관리자 역할로만 제한해야 합니다. | `microsoft.graph/policies/authorizationpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 권한 부여 정책은 보안 그룹 생성을 관리자로 제한해야 합니다. | `microsoft.graph/policies/authorizationpolicy` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Microsoft Entra 테넌트는 디바이스를 등록하거나 조인하기 위해 다중 인증이 필요합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Entra ID 디렉터리 역할에는 2~4명의 글로벌 관리자가 있어야 합니다. | `microsoft.graph/directoryrole` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Entra ID 그룹 설정은 그룹 생성을 관리자로 제한해야 합니다. | `microsoft.graph/organization` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 활동 로그에 대한 진단 설정이 구성되어 있어야 합니다. | `microsoft.insights/diagnosticsettings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 정책 할당 생성을 위한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 정책 할당 삭제에 대한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 네트워크 보안 그룹 작업 생성 또는 업데이트에 대한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 네트워크 보안 그룹 삭제에 대한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 보안 솔루션 생성 또는 업데이트에 대한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure 구독에는 보안 솔루션 삭제에 대한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 SQL Server 방화벽 규칙 생성 또는 업데이트를 위한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 SQL Server 방화벽 규칙을 삭제하기 위한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 퍼블릭 IP 주소 생성 또는 업데이트 작업에 대해 활동 로그 알림이 구성되어 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 퍼블릭 IP 주소 삭제에 대한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 서비스 상태 인시던트에 대한 활동 로그 알림이 있어야 합니다. | `microsoft.insights/activitylogalerts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 하나 이상의 Application Insights 구성 요소가 구성되어 있어야 합니다. | `microsoft.insights/components` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Key Vaults에는 소프트 삭제 및 제거 보호가 활성화되어 있어야 합니다. | `microsoft.keyvault/vaults` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Key Vaults에는 역할 기반 액세스 제어가 활성화되어 있어야 합니다. | `microsoft.keyvault/vaults` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| 프라이빗 엔드포인트를 사용할 때는 Azure Key Vault에 퍼블릭 네트워크 액세스가 비활성화되어 있어야 합니다. | `microsoft.keyvault/vaults` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Key Vault는 프라이빗 엔드포인트를 사용해야 합니다. | `microsoft.keyvault/vaults` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Key Vaults에는 제거 보호가 활성화되어 있어야 합니다. | `microsoft.keyvault/vaults` | Azure 기본 모범 사례 |
| Azure Key Vault는 네트워크 액세스를 제한해야 합니다. | `microsoft.keyvault/vaults` | Azure 기본 모범 사례 |
| Azure Key Vaults에는 AuditEvent 로깅이 활성화되어 있어야 합니다. | `microsoft.keyvault/vaults` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| RBAC 볼트의 Azure Key Vault 키에는 만료 날짜가 설정되어 있어야 합니다. | `microsoft.keyvault/vaults/keys` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| 비 RBAC 볼트의 Azure Key Vault 키에는 만료 날짜가 설정되어 있어야 합니다. | `microsoft.keyvault/vaults/keys` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| RBAC 지원 저장소의 Azure Key Vault 보안 암호에는 만료 날짜가 설정되어 있어야 합니다. | `microsoft.keyvault/vaults/secrets` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| 비 RBAC 볼트의 Azure Key Vault 보안 암호에는 만료 날짜가 설정되어 있어야 합니다. | `microsoft.keyvault/vaults/secrets` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Key Vault 키에는 자동 교체가 활성화되어 있어야 합니다. | `microsoft.keyvault/vaults/keys` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure 네트워크 보안 그룹은 인터넷으로부터의 인바운드 RDP 액세스를 제한해야 합니다. | `microsoft.network/networksecuritygroups` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 네트워크 보안 그룹은 인터넷으로부터의 인바운드 UDP 액세스를 제한해야 합니다. | `microsoft.network/networksecuritygroups` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 네트워크 보안 그룹은 인터넷으로부터의 인바운드 HTTP 액세스를 제한해야 합니다. | `microsoft.network/networksecuritygroups` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Application Gateway 서브넷에는 무제한 NSG 액세스 권한이 없어야 합니다. | `microsoft.network/networksecuritygroups` | Azure 기본 모범 사례 |
| Azure 네트워크 보안 그룹에는 명시적 거부 규칙이 있어야 합니다. | `microsoft.network/networksecuritygroups` | Azure 기본 모범 사례 |
| Azure 네트워크 보안 그룹은 제한된 포트에 대한 무제한 인바운드 액세스를 허용해서는 안 됩니다. | `microsoft.network/networksecuritygroups` | Azure 기본 모범 사례 |
| Azure Network Watcher 흐름 로그에는 Log Analytics로 전송된 트래픽 분석과 함께 가상 네트워크 흐름 로깅이 활성화되어 있어야 합니다. | `microsoft.network/networkwatchers/flowlogs` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 네트워크 보안 그룹은 인터넷에서 SSH 액세스를 제한해야 합니다. | `microsoft.network/networksecuritygroups` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Azure Bastion 호스트가 하나 이상 있어야 합니다. | `microsoft.network/bastionhosts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure 구독에는 서버용 Microsoft Defender가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| 머신에는 Microsoft Defender for Cloud에 배포된 정상적인 취약성 평가 솔루션이 있어야 합니다. | `microsoft.security/assessments` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Microsoft Defender for Cloud와 엔드포인트 보호 통합이 활성화되어 있어야 합니다. | `microsoft.security/settings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 서버용 Microsoft Defender에서 활성화된 시스템에 대한 에이전트 없는 스캔이 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 서버용 Defender에서 파일 무결성 모니터링이 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 컨테이너용 Microsoft Defender가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Microsoft Defender for Storage가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Microsoft Defender for App Service가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Azure Cosmos DB용 Microsoft Defender가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure 구독에는 오픈 소스 관계형 데이터베이스에 대해 Microsoft Defender가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Azure SQL Databases용 Microsoft Defender가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Microsoft Defender for SQL Servers on Machines가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Microsoft Defender for Key Vault가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 Resource Manager용 Microsoft Defender가 활성화되어 있어야 합니다. | `microsoft.security/pricings` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| 가상 머신에는 Microsoft Defender for Cloud에서 정상으로 보고한 시스템 업데이트 평가가 있어야 합니다. | `microsoft.security/assessments` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Defender for Cloud 보안 연락처는 소유자 역할에 알림을 알려야 합니다. | `microsoft.security/securitycontacts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Microsoft Defender for Cloud 보안 연락처에는 추가 이메일 주소가 구성되어 있어야 합니다. | `microsoft.security/securitycontacts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 보안 연락처에는 충분히 포괄적인 최소 심각도로 알림 이메일 알림이 활성화되어 있어야 합니다. | `microsoft.security/securitycontacts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure 보안 연락처에는 위험 수준이 구성된 공격 경로 이메일 알림이 활성화되어 있어야 합니다. | `microsoft.security/securitycontacts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure 구독에는 IoT용 Microsoft Defender가 활성화되어 있어야 합니다. | `microsoft.security/iotsecuritysolutions` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure SQL 서버에는 퍼블릭 네트워크 액세스가 비활성화되어 있어야 합니다. | `microsoft.sql/servers` | Azure 기본 모범 사례 |
| SQL 서버에는 Azure Active Directory 관리자가 구성되어 있어야 합니다. | `microsoft.sql/servers` | Azure 기본 모범 사례 |
| Azure SQL 데이터베이스에는 지리 중복 백업이 활성화되어 있어야 합니다. | `microsoft.sql/servers/databases` | Azure 기본 모범 사례 |
| Azure SQL 서버는 기본 관리자 계정 이름을 사용해서는 안 됩니다. | `microsoft.sql/servers` | Azure 기본 모범 사례 |
| Azure SQL 관리형 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다. | `microsoft.sql/managedinstances` | Azure 기본 모범 사례 |
| Azure Storage 계정은 암호화에 고객 관리형 키를 사용해야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정 파일 서비스에는 파일 공유에 대해 소프트 삭제가 활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts/fileservices` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정 파일 공유는 SMB 프로토콜 버전을 SMB 3.1.1로 제한해야 합니다. | `microsoft.storage/storageaccounts/fileservices` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure Storage 계정은 파일 공유에 안전한 SMB 채널 암호화 알고리즘을 사용해야 합니다. | `microsoft.storage/storageaccounts/fileservices` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에는 키 교체 미리 알림이 구성되어 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에 공유 키 액세스가 비활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정은 액세스를 위해 프라이빗 엔드포인트를 사용해야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에는 퍼블릭 네트워크 액세스가 비활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에는 거부하도록 기본 네트워크 액세스가 설정되어 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| 스토리지 계정은 Azure 포털에서 Microsoft Entra 권한 부여로 기본 설정되어 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에는 보안 전송이 필요합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정은 신뢰할 수 있는 Azure 서비스가 네트워크 규칙을 우회하도록 허용해야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure Storage 계정은 필요한 최소 TLS 버전으로 구성해야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에는 테넌트 간 복제가 비활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에는 익명 Blob 액세스가 비활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정은 영구 Blob 삭제를 제한해야 합니다. | `microsoft.storage/storageaccounts/blobservices` | Azure 기본 모범 사례 |
| 활동 로그가 포함된 Azure 스토리지 계정은 고객 관리형 키로 암호화해야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정 Blob 서비스에는 Blob 소프트 삭제가 활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts/blobservices` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정 Blob 서비스에는 버전 관리가 활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts/blobservices` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정 Blob 서비스에는 Blob 및 컨테이너 소프트 삭제가 활성화되어 있어야 합니다. | `microsoft.storage/storageaccounts/blobservices` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정에는 Azure Resource Manager 삭제 잠금이 적용되어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

| 컨트롤 제목 | 리소스 유형 | 표준 |
| --- | --- | --- |
| Azure Storage 계정에는 ReadOnly 리소스 관리자 잠금이 있어야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Storage 계정은 지리 중복 스토리지를 사용해야 합니다. | `microsoft.storage/storageaccounts` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |
| Azure Function 앱은 관리 액세스를 제한해야 합니다. | `microsoft.web/sites/config` | Azure 기본 모범 사례 |
| Azure Functions는 익명 HTTP 트리거 호출을 허용해서는 안 됩니다. | `microsoft.web/sites/functions` | Azure 기본 모범 사례 |
| Azure App Service 웹 앱 및 함수 앱은 지원되지 않는 런타임 버전을 사용해서는 안 됩니다. | `microsoft.web/sites` | Azure 기본 모범 사례 |
| 프리미엄 또는 전용 플랜의 Azure Function 앱은 가상 네트워크와 통합되어야 합니다. | `microsoft.web/sites` | Azure 기본 모범 사례 |
| Azure App Service 웹 앱에는 진단 설정에서 HTTP 로그가 활성화되어 있어야 합니다. | `microsoft.web/sites` | CIS Microsoft Azure Foundations 벤치마크 v4.0 |

## Security Hub CSPM에서 Microsoft Azure 커넥터 삭제

AWS Security Hub CSPM에서 Microsoft Azure 커넥터를 생성한 후 언제든지 삭제할 수 있습니다. 커넥터를 삭제하면 Security Hub CSPM은 Azure 환경에 대한 태세 관리 검사 및 취약성 모니터링 수행을 중지합니다. Security Hub CSPM은 환경에 대한 새 결과 생성도 중지합니다. 기존 조사 결과는 90일 동안 보존됩니다. 리소스 인벤토리는 커넥터가 삭제되고 90일 후에 제거될 때와 동일하게 유지됩니다.

커넥터를 삭제할 때 다음 사항에 유의하세요.

- Security Hub CSPM은 Azure 환경에서 Azure 애플리케이션 등록 및 Event Hub 인프라를 삭제하지 않습니다. Microsoft Azure에서 직접 수동으로 삭제해야 합니다. 자세한 내용은 Microsoft Azure 설명서의 애플리케이션 제거를 참조하세요.
- 커넥터가 고객 관리형 커넥터이고 서비스 연결 커넥터도 있는 경우 고객 관리형 커넥터를 삭제해도 서비스 연결 커넥터에는 영향을 주지 않습니다. Security Hub CSPM은 서비스 연결 커넥터를 통해 태세 관리 조사 결과를 계속 수신합니다.
- 기존 결과는 3~5일 이내에 아카이브된 상태로 전환되며 90일 보존 기간 후에 삭제됩니다.

Azure 커넥터를 삭제하려면

1. Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 통합을 선택합니다.
3. 커넥터를 선택합니다.
4. 삭제를 선택합니다.
5. 메시지가 표시되면 커넥터를 삭제할지 확인합니다.

삭제 후 설정 중에 생성된 Azure 리소스를 선택적으로 정리할 수 있습니다.

- Microsoft Entra ID에서 앱 등록을 삭제합니다.
- Event Hub 네임스페이스 및 리소스 그룹을 삭제합니다.
- 활동 로그 및 Entra ID 감사 로그를 내보내는 진단 설정을 제거합니다.

# Security Hub CSPM에서 조사 결과 생성 및 업데이트

AWS Security Hub CSPM에서 결과는 보안 검사 또는 보안 관련 탐지에 대한 관찰 가능한 레코드입니다. 조사 결과는 다음 소스 중 하나에서 시작될 수 있습니다.

- Security Hub CSPM의 제어에 대한 보안 검사.
- 다른 와의 통합 AWS 서비스.
- 서드 파티 제품과의 통합.
- 사용자 지정 통합.

Security Hub CSPM은 모든 소스로부터의 조사 결과를 AWS Security Finding Format(ASFF)이라고 하는 표준 구문 및 형식으로 정규화합니다. 개별 ASFF 필드에 대한 설명을 포함하여 이 형식에 대한 자

세한 내용은 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요. 교차 리전 집계를 활성화할 경우, Security Hub CSPM은 연결된 리전의 새로운 조사 결과 및 업데이트된 조사 결과를 집계 영역으로 자동 집계합니다. 자세한 내용은 Security Hub CSPM의 교차 리전 집계 이해 단원을 참조하십시오.

조사 결과가 생성된 후 다음과 같이 업데이트할 수 있습니다.

- 조사 결과 공급자는 Security Hub CSPM API의 BatchImportFindings 작업을 사용하여 조사 결과에 대한 일반 정보를 업데이트할 수 있습니다. 조사 결과 공급자는 자신이 생성한 조사 결과만 업데이트할 수 있습니다.
- 고객은 Security Hub CSPM 콘솔 또는 Security Hub CSPM API의 BatchUpdateFindings 작업을 사용하여 조사의 상태를 조사 결과로 업데이트할 수 있습니다. SIEM, 티켓팅, 인시던트 관리, SOAR 또는 기타 유형의 도구가 고객을 대신하여 `BatchUpdateFindings` 작업을 사용할 수도 있습니다.

조사 결과 노이즈를 줄이고 개별 조사 결과의 추적 및 분석을 간소화하기 위해 Security Hub CSPM은 최근에 업데이트되지 않은 조사 결과를 자동으로 삭제합니다. Security Hub CSPM이 이 작업을 수행하는 시기는 조사 결과가 활성 상태인지 아니면 보관된 상태인지에 따라 달라집니다.

- 활성 조사 결과는 레코드 상태(`RecordState`)가 `ACTIVE`인 조사 결과입니다. Security Hub CSPM은 활성 조사 결과를 90일 동안 저장합니다. 활성 조사 결과가 90일 동안 업데이트되지 않은 경우 해당 조사 결과는 만료되고 Security Hub CSPM이 영구적으로 삭제합니다.
- 보관된 조사 결과 레코드 상태(`RecordState`)가 `ARCHIVED`인 조사 결과입니다. Security Hub CSPM은 보관된 조사 결과를 30일 동안 저장합니다. 보관된 조사 결과가 30일 동안 업데이트되지 않은 경우 해당 조사 결과는 만료되고 Security Hub CSPM이 영구적으로 삭제합니다.

Security Hub CSPM이 제어에 대한 보안 검사에서 생성하는 조사 결과인 제어 조사 결과의 경우 Security Hub CSPM은 조사 결과의 `UpdatedAt` 필드 값을 기반으로 조사 결과가 만료되었는지 여부를 결정합니다. 활성 조사 결과에서 이 값이 90일을 초과하는 경우 Security Hub CSPM은 해당 조사 결과를 영구적으로 삭제합니다. 보관된 조사 결과에서 이 값이 30일을 초과하는 경우 Security Hub CSPM은 해당 조사 결과를 영구적으로 삭제합니다.

다른 모든 유형의 조사 결과의 경우 Security Hub CSPM은 조사 결과의 `ProcessedAt` 및 `UpdatedAt` 필드 값을 기반으로 조사 결과가 만료되었는지 여부를 결정합니다. Security Hub CSPM은 이러한 필드의 값을 비교하여 최신 필드를 결정합니다. 활성 조사 결과에서 최신 값이 90일을 초과하는 경우 Security Hub CSPM은 해당 조사 결과를 영구적으로 삭제합니다. 보관된 조사 결과에서 최신 값이 30일을 초과하는 경우 Security Hub CSPM은 해당 조사 결과를 영구적으로 삭제합니다. 조사 결과 공급자는 Security Hub CSPM API의 BatchImportFindings 작업을 사용하여 하나 이상의 조사 결과에서 `UpdatedAt` 필드 값을 변경할 수 있습니다.

조사 결과를 장기 보존하려면 조사 결과를 S3 버킷으로 내보낼 수 있습니다. 이 작업은 Amazon EventBridge 규칙과 함께 사용자 지정 작업을 사용하여 수행할 수 있습니다. 자세한 내용은 자동 응답 및 문제 해결을 위해 EventBridge 사용 단원을 참조하십시오.

주제


- 조사 결과 공급자에 대한 BatchImportFindings
- 고객에 대한 BatchUpdateFindings
- Security Hub CSPM에서 조사 결과 세부 정보 및 기록 검토
- Security Hub CSPM에서 조사 결과 필터링
- Security Hub CSPM에서 조사 결과 그룹화
- Security Hub CSPM에서 조사 결과의 워크플로 상태 설정
- 사용자 지정 Security Hub CSPM 작업으로 조사 결과 전송
- AWS 보안 조사 결과 형식(ASFF)


## 조사 결과 공급자에 대한 BatchImportFindings

조사 결과 공급자는 BatchImportFindings 작업을 사용하여 AWS Security Hub CSPM에서 새로운 조사 결과를 생성할 수 있습니다. 또한 이 작업을 사용하여 자신이 생성한 조사 결과를 업데이트할 수도 있습니다. 조사 결과 공급자는 자신이 생성하지 않은 조사 결과를 업데이트할 수 없습니다.

고객, SIEM, 티켓팅, SOAR 및 기타 유형의 도구는 반드시 BatchUpdateFindings 작업을 사용하여 조사 결과 공급자의 조사 결과에 대한 조사와 관련된 업데이트를 수행해야 합니다. 자세한 내용은 the section called “고객에 대한 BatchUpdateFindings” 단원을 참조하십시오.

Security Hub CSPM은 조사 결과를 생성 또는 업데이트하라는 `BatchImportFindings` 요청을 받을 때마다 Amazon EventBridge에서 자동으로 Security Hub Findings - Imported 이벤트를 생성합니다. 해당 이벤트에 대해 자동 작업을 수행할 수 있습니다. 자세한 내용은 the section called “자동 응답 및 해결” 단원을 참조하십시오.

### `BatchImportFindings` 사용을 위한 사전 조건

`BatchImportFindings`은(는) 다음 중 하나에 의해 직접 호출되어야 합니다.

- 조사 결과와 연결된 계정. 관련 계정의 식별자는 조사 결과에 대한 `AwsAccountId` 속성의 값과 일치해야 합니다.
- 공식 Security Hub CSPM 파트너 통합을 위해 허용 목록에 있는 계정.

Security Hub CSPM은 Security Hub CSPM이 활성화된 계정에 대한 조사 결과 업데이트만 수락할 수 있습니다. 조사 결과 공급자도 활성화해야 합니다. Security Hub CSPM이 비활성화되거나 조사 결과 공급자 통합이 활성화되지 않은 경우, 조사 결과가 `InvalidAccess` 오류와 함께 `FailedFindings` 목록에 반환됩니다.

### 조사 결과 생성 또는 갱신 여부 결정

조사 결과를 생성할지 또는 업데이트할지 여부를 결정하기 위해 Security Hub CSPM은 `ID` 필드를 확인합니다. `ID` 값이 기존 조사 결과와 일치하지 않으면 Security Hub CSPM은 새로운 조사 결과를 생성합니다.

`ID`가 기존 조사 결과와 일치하는 경우, Security Hub CSPM은 `UpdatedAt` 필드에 업데이트가 있는지 확인하고 다음과 같이 진행합니다.

- 업데이트의 `UpdatedAt`가 기존 조사 결과의 `UpdatedAt`와 일치하거나 이전인 경우 Security Hub CSPM은 업데이트 요청을 무시합니다.
- 업데이트의 `UpdatedAt`가 기존 조사 결과의 `UpdatedAt` 이후인 경우 Security Hub CSPM은 기존 조사 결과를 업데이트합니다.

### **`BatchImportFindings`**에서 조사 결과 업데이트에 관한 제한

조사 결과 공급자는 기존 조사 결과의 다음 속성을 업데이트하는 데 `BatchImportFindings`을(를) 사용할 수 없습니다.

- `Note`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

Security Hub CSPM은 이러한 속성에 대한 `BatchImportFindings` 요청에 제공된 모든 콘텐츠를 무시합니다. 고객 또는 고객을 대신하여 활동하는 엔티티(예: 티켓팅 도구)는 `BatchUpdateFindings`을(를) 사용하여 이러한 속성을 업데이트할 수 있습니다.

### FindingProviderFields(으)로 조사 결과 업데이트

또한 결과 공급자는 AWS Security Finding Format(ASFF)에서 다음과 같은 최상위 속성을 업데이트하는 `BatchImportFindings` 데를 사용해서는 안 됩니다.

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

대신, 조사 결과 공급자는 FindingProviderFields 객체를 사용하여 이러한 속성에 대한 값을 제공해야 합니다.

예제

```
"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" ]
}
```

BatchImportFindings 요청의 경우, Security Hub CSPM은 최상위 속성 및 FindingProviderFields의 값을 다음과 같이 처리합니다.

(선호)**BatchImportFindings**은(는) **FindingProviderFields**의 속성 값을 제공하지만 해당하는 최상위 속성에 대한 값은 제공하지 않습니다.

예를 들어, BatchImportFindings은(는) FindingProviderFields.Confidence을 제공하지만 Confidence을 제공하지는 않습니다. BatchImportFindings 요청에는 이 옵션을 사용하는 것이 좋습니다.

Security Hub CSPM은 FindingProviderFields의 속성 값을 업데이트합니다.

이는 BatchUpdateFindings에 의해 속성을 아직 업데이트하지 않은 경우에만 최상위 속성에 값을 복제합니다.

**BatchImportFindings**은(는) 최상위 속성에 대한 값을 제공하지만 **FindingProviderFields**에서 해당하는 속성의 값은 제공하지 않습니다.

예를 들어, BatchImportFindings은(는) FindingProviderFields.Confidence을(를) 제공하지만 Confidence을(를) 제공하지는 않습니다.

Security Hub CSPM은 이 값을 사용하여 FindingProviderFields의 속성을 업데이트합니다. 이는 기존 값을 모두 덮어씁니다.

Security Hub CSPM은 속성이 BatchUpdateFindings에 의해 아직 업데이트되지 않은 경우에만 최상위 속성을 업데이트합니다.

**BatchImportFindings**은(는) 최상위 속성과 **FindingProviderFields**의 해당 속성 모두에 대한 값을 제공합니다.

예를 들어, BatchImportFindings은(는) Confidence 및 FindingProviderFields.Confidence을(를) 모두 제공합니다.

새로운 조사 결과의 경우, Security Hub CSPM은 FindingProviderFields의 값을 사용하여 최상위 속성과 FindingProviderFields의 해당 속성을 모두 채웁니다. 이는 입력된 최상위 속성 값은 사용하지 않습니다.

기존 조사 결과의 경우, Security Hub CSPM은 두 값을 모두 사용합니다. 하지만 BatchUpdateFindings에서 속성을 아직 업데이트하지 않은 경우에만 최상위 속성 값을 업데이트합니다.

## 고객에 대한 BatchUpdateFindings

AWS Security Hub CSPM 고객과 이를 대신하여 활동하는 엔터티는 BatchUpdateFindings 작업을 사용하여 조사 결과 공급자의 Security Hub CSPM 조사 결과 처리와 관련된 정보를 업데이트할 수 있습니다. 고객은 이 작업을 직접 사용할 수 있습니다. SIEM, 티켓팅, 인시던트 관리 및 SOAR 도구도 고객을 대신하여 이 작업을 사용할 수 있습니다.

새로운 조사 결과를 생성하는 데는 BatchUpdateFindings를 사용할 수 없습니다. 하지만 한 번에 최대 100개의 기존 조사 결과를 업데이트하는 데 사용할 수 있습니다. BatchUpdateFindings 요청에서 업데이트할 조사 결과, 조사 결과에 대해 업데이트할 AWS Security Finding Format(ASFF) 필드, 필드에 대한 새 값을 지정합니다. 그런 다음 Security Hub CSPM은 요청에 지정된 대로 조사 결과를 업

데이트합니다. 이 프로세스는 몇 분 정도 걸릴 수 있습니다. BatchUpdateFindings 작업을 사용하여 조사 결과를 업데이트하는 경우 업데이트는 조사 결과의 UpdatedAt 필드의 기존 값에 영향을 주지 않습니다.

Security Hub CSPM은 조사 결과 업데이트를 위한 BatchUpdateFindings 요청을 받을 때마다 Amazon EventBridge에서 자동으로 Security Hub Findings – Imported 이벤트를 생성합니다. 선택적으로 이 이벤트를 사용하여 지정된 조사 결과에 대해 자동화된 작업을 수행할 수 있습니다. 자세한 내용은 the section called “자동 응답 및 해결” 단원을 참조하십시오.

## BatchUpdateFindings에 사용 가능한 필드

Security Hub CSPM 관리자 계정에 로그인한 경우, BatchUpdateFindings를 사용하여 관리자 계정 또는 멤버 계정에서 생성된 조사 결과를 업데이트할 수 있습니다. 멤버 계정은 자신의 계정만의 조사 결과를 업데이트하는 데 BatchUpdateFindings을(를) 사용할 수 있습니다.

고객은 BatchUpdateFindings만 사용하여 다음 필드와 객체를 업데이트할 수 있습니다.

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

## BatchUpdateFindings에 대한 액세스 구성

를 사용하여 결과 필드 및 필드 값을 BatchUpdateFindings 업데이트하는 액세스를 제한하도록 AWS Identity and Access Management (IAM) 정책을 구성할 수 있습니다.

액세스를 BatchUpdateFindings로 제한하는 문에는 다음 값을 사용하세요.

- Action은(는) securityhub:BatchUpdateFindings
- Effect은(는) Deny
- Condition의 경우, 다음을 기준으로 BatchUpdateFindings 요청을 거부할 수 있습니다.

- 조사 결과에 특정 필드가 포함됩니다.
- 조사 결과에 특정 필드 값이 포함됩니다.

조건 키

액세스를 BatchUpdateFindings로 제한하기 위한 조건 키입니다.

ASFF 필드

ASFF 필드의 조건 키는 다음과 같습니다.

```
securityhub:ASFFSyntaxPath/<fieldName>
```

*<fieldName>*을(를) ASFF 필드로 대체하세요. BatchUpdateFindings에 대한 액세스를 구성할 때는 상위 수준 필드 대신 IAM 정책에 하나 이상의 특정 ASFF 필드를 포함하세요. 예를 들어, Workflow.Status 필드에 대한 액세스를 제한하려면 Workflow 상위 수준 필드 대신 정책에 securityhub:ASFFSyntaxPath/Workflow.Status을(를) 포함해야 합니다.

필드에 대한 모든 업데이트 허용 안 함

사용자가 특정 필드를 업데이트하지 못하게 하려면 다음과 같은 조건을 사용하세요.

```
 "Condition": {
                "Null": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "false"
               }
}
```

예를 들어, 다음 문은 Workflow.Status 조사 결과의 필드를 업데이트하는 데 BatchUpdateFindings을(를) 사용할 수 없음을 나타냅니다.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
        "Null": {
            "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
        }
```

```
    }
}
```

특정 필드 값 허용 안 함

사용자가 필드를 특정 값으로 설정하는 것을 방지하려면 다음과 같은 조건을 사용하세요.

```
"Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
                }
}
```

예를 들어, 다음 문은 Workflow.Status을(를) SUPPRESSED(으)로 설정하는 데 BatchUpdateFindings을(를) 사용할 수 없음을 나타냅니다.

```
{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
}
```

허용되지 않는 값 목록을 입력할 수도 있습니다.

```
 "Condition": {
                "StringEquals": {
                    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
 "<fieldValue2>", "<fieldValuen>" ]
                }
}
```

예를 들어, 다음 문은 Workflow.Status을(를) RESOLVED 또는 SUPPRESSED 중 하나로 설정하는 데 BatchUpdateFindings을(를) 사용할 수 없음을 나타냅니다.

```
{
    "Sid": "VisualEditor0",
```

```
    "Effect": "Deny",
    "Action": "securityhub:BatchUpdateFindings",
    "Resource": "*",
    "Condition": {
    "StringEquals": {
        "securityhub:ASFFSyntaxPath/Workflow.Status": [
            "RESOLVED",
            "NOTIFIED"
        ]
    }
}
```

## Security Hub CSPM에서 조사 결과 세부 정보 및 기록 검토

AWS Security Hub CSPM에서 결과는 보안 검사 또는 보안 관련 탐지에 대한 관찰 가능한 레코드입니다. Security Hub CSPM은 제어의 보안 검사를 완료하고 통합 AWS 서비스 또는 서드 파티 제품에서 조사 결과를 수집할 때 조사 결과를 생성합니다. 각 조사 결과에는 변경 기록과 심각도 등급 및 영향을 받는 리소스에 대한 정보와 같은 기타 세부 정보가 포함됩니다.

Security Hub CSPM 콘솔에서 또는 Security Hub CSPM API 및 AWS CLI를 통해 프로그래밍 방식으로 개별 조사 결과의 기록 및 기타 세부 정보를 검토할 수 있습니다.

분석을 간소화하는 데 도움이 되도록 Security Hub CSPM 콘솔은 특정 조사 결과를 선택할 때 조사 결과 패널을 표시합니다. 이 패널에는 다양한 조사 결과의 세부 정보를 볼 수 있는 다양한 메뉴 및 탭이 포함되어 있습니다.

실행 메뉴

이 메뉴에서 조사 결과의 전체 JSON을 검토하거나 메모를 추가할 수 있습니다. 조사 결과에는 한 번에 하나의 메모만 연결할 수 없습니다. 또한 이 메뉴는 조사 결과의 워크플로 상태를 설정하거나 Amazon EventBridge의 사용자 지정 작업에 조사 결과를 전송하는 옵션을 제공합니다.

메뉴 조사

이 메뉴에서 Amazon Detective의 조사 결과를 조사할 수 있습니다. Detective는 조사 결과에서 IP 주소 및 AWS 사용자와 같은 개체를 추출하고 활동을 시각화합니다. 엔티티 활동을 시작점으로 사용하여 조사 결과의 원인과 영향을 조사할 수 있습니다.

개요 탭

이 탭은 조사 결과에 대한 요약을 제공합니다. 예를 들어 조사 결과가 생성 및 마지막으로 업데이트된 시점, 조사 결과가 있는 계정 및 조사 결과의 소스를 확인할 수 있습니다. 제어 조사 결과의 경우

이 탭에는 연결된 AWS Config 규칙 이름과 Security Hub CSPM 설명서의 문제 해결 지침에 대한 링크도 표시됩니다.

개요 탭의 리소스 스냅샷에서 조사 결과에 관련된 리소스에 대한 간략한 개요를 확인할 수 있습니다. 일부 리소스의 경우 여기에는 관련 AWS 서비스 콘솔의 영향을 받는 리소스에 직접 연결되는 리소스 열기 옵션이 포함됩니다. 기록 스냅샷은 기록이 추적되는 가장 최근 날짜에 조사 결과에 대한 최대 2개의 변경 사항을 표시합니다. 예를 들어, 어제 한 번 변경하고 오늘 다시 한 번 변경한 경우, 스냅샷에는 오늘의 변경 사항만 표시됩니다. 이전 항목을 보려면 기록 탭으로 전환합니다.

규정 준수 행이 확장되면서 세부 정보가 표시됩니다. 예를 들어, 제어에 파라미터가 포함된 경우, Security Hub CSPM이 보안 검사를 실행할 때 현재 사용하는 파라미터 값을 검토할 수 있습니다.

리소스 탭

이 탭은 조사 결과에 관련된 리소스에 대한 세부 정보를 제공합니다. 리소스를 소유한 계정에 로그인한 경우 해당 AWS 서비스 콘솔에서 리소스를 검토할 수 있습니다. 리소스 소유자가 아닌 경우이 탭에는 소유자의 AWS 계정 ID가 표시됩니다.

세부 정보 행에는 조사 결과의 리소스별 세부 정보가 표시됩니다. 이 행은 조사 결과의 ResourceDetails 섹션을 JSON 형식으로 보여줍니다.

태그 행에는 조사 결과와 관련된 리소스에 할당된 태그 키 및 값이 표시됩니다. 태깅 API의 GetResources 작업에서 지원되는 리소스에 AWS Resource Groups 태그를 지정할 수 있습니다. Security Hub CSPM은 새로운 또는 업데이트된 조사 결과를 처리할 때 서비스 연결 역할을 통해 이 작업을 직접 호출하고, AWS Security Finding Format(ASFF) `Resource.Id` 필드에 리소스 ARN이 입력되어 있으면 리소스 태그를 검색합니다. Security Hub CSPM은 잘못된 리소스 ID를 무시합니다. 조사 결과에 리소스 태그를 포함하는 방법에 대한 자세한 내용은 Tags 섹션을 참조하세요.

기록 탭

이 탭은 조사 결과의 기록을 추적합니다. 조사 결과 기록은 활성 및 보관된 조사 결과 기록에 사용할 수 있습니다. 이는 ASFF 필드 변경 내용, 변경 시점, 해당 사용자를 포함하여 시간이 지남에 따라 조사 결과에 적용된 변경 사항에 대한 불변의 추적을 제공합니다. 이 탭의 각 페이지에는 최대 20개의 변경 사항이 표시됩니다. 최신 변경 사항이 먼저 표시됩니다.

활성 조사 결과의 경우 조사 결과 기록을 최대 90일 동안 사용할 수 있습니다. 보관된 조사 결과의 경우 조사 결과 기록을 최대 30일 동안 사용할 수 있습니다. 조사 결과 기록에는 수동으로 또는 Security Hub CSPM 자동화 규칙을 통해 자동으로 수행한 변경 사항이 포함됩니다. 여기에는 `CreatedAt` 및 `UpdatedAt`와 같은 최상위 타임스탬프 필드에 대한 변경 사항은 포함되지 않습니다.

Security Hub CSPM 관리자 계정으로 로그인한 경우, 조사 결과 기록에는 관리자 계정 및 모든 멤버 계정이 포함됩니다.

위협 탭

이 탭에는 위협 유형 및 리소스가 대상인지 또는 공격자인지 여부를 포함하여 ASFF의 Action, Malware 및 ProcessDetails 객체에서 얻은 데이터가 포함됩니다. 이러한 세부 정보는 일반적으로 Amazon GuardDuty에서 시작된 조사 결과에 적용됩니다.

취약성 탭

이 탭은 조사 결과와 관련된 악용 또는 사용 가능한 수정 사항이 있는지 여부를 포함하여 ASFF의 Vulnerability 객체의 데이터를 표시합니다. 이러한 세부 정보는 일반적으로 Amazon Inspector에서 시작된 조사 결과에 적용됩니다.

각 탭의 행에는 복사 또는 필터 옵션이 포함됩니다. 예를 들어, 워크플로 상태가 알림인 조사 결과의 패널을 여는 경우, 워크플로 상태 행 옆에 있는 필터 옵션을 선택할 수 있습니다. 이 값을 사용하여 모든 조사 결과 표시를 선택하면 Security Hub CSPM이 조사 결과 테이블을 필터링하여 워크플로 상태가 동일한 조사 결과만 표시합니다.

## 조사 결과 세부 정보 및 기록 검토

원하는 방법을 선택하고 단계에 따라 Security Hub CSPM의 조사 결과 세부 정보를 검토하세요.

교차 리전 집계를 활성화하고 집계 리전에 로그인하는 경우, 조사 결과에는 집계 리전 및 연결된 리전의 조사 결과 데이터가 포함됩니다. 다른 리전에서는 조사 결과 데이터가 해당 리전에만 적용됩니다. 교차 리전 집계 활성화에 대한 자세한 내용은 the section called “리전 간 데이터 집계” 섹션을 참조하세요.

Security Hub CSPM console

조사 결과 세부 정보 및 기록 검토

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 조사 결과 목록을 표시하려면 다음 중 하나를 수행하세요.
   - 탐색 창에서 조사 결과를 선택합니다. 필요에 따라 검색 필터를 추가하여 조사 결과 목록의 범위를 좁힙니다.
   - 탐색 창에서 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.

- 탐색 창에서 통합을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.
- 탐색 창에서 제어를 선택합니다.

3. 조사 결과를 선택합니다. 조사 결과 패널에 조사 결과의 세부 정보가 표시됩니다.
4. 조사 결과 패널에서 다음 작업 중 하나를 수행합니다.

- 조사 결과의 특정 세부 정보를 검토하려면 탭을 선택합니다.
- 조사 결과에 대한 조치를 취하려면 작업 메뉴에서 옵션을 선택합니다.
- Amazon Detective에서 조사 결과를 조사하려면 조사 옵션을 선택합니다.

> **Note**
>
> 를와 통합 AWS Organizations 하고 멤버 계정에 로그인한 경우 결과 패널에 계정 이름이 포함됩니다. Organizations를 통하지 않고 수동으로 초대된 멤버 계정의 경우, 조사 결과 패널에 계정 ID만 포함됩니다.

### Security Hub CSPM API

Security Hub CSPM API의 GetFindings 작업을 사용하거나를 사용하는 경우 get-findings 명령을 AWS CLI실행합니다. `Filters` 파라미터에 하나 이상의 값을 제공하여 검색할 조사 결과의 범위를 좁힐 수 있습니다.

결과의 양이 너무 많으면 `MaxResults` 파라미터를 사용하여 조사 결과를 지정된 수로 제한하고 `NextToken` 파라미터를 사용하여 조사 결과의 페이지를 매길 수 있습니다. `SortCriteria` 파라미터를 사용해 특정 필드를 기준으로 조사 결과를 정렬할 수 있습니다.

예를 들어 다음 AWS CLI 명령은 지정된 필터 기준과 일치하는 결과를 검색하고 `LastObservedAt` 필드를 기준으로 결과를 내림차순으로 정렬합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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
```

조사 결과 기록을 검토하려면 GetFindingHistory 작업을 사용합니다. 를 사용하는 경우 get-finding-history 명령을 AWS CLI실행합니다. `ProductArn` 및 `Id` 필드를 사용하여 기록을 가져오려는 조사

결과를 식별합니다. 이러한 필드에 대한 자세한 내용은 AwsSecurityFindingIdentifier 섹션을 참조하세요. 각 요청은 하나의 조사 결과에 대한 기록만 검색할 수 있습니다.

예를 들어 다음 AWS CLI 명령은 지정된 결과에 대한 기록을 검색합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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

`Get-SHUBFinding` cmdlet을 사용하세요. 선택적으로 `Filter` 파라미터를 채워 검색할 조사 결과의 범위를 좁힙니다.

예를 들어 다음 cmdlet은 지정된 필터와 일치하는 조사 결과를 검색합니다.

```
Get-SHUBFinding -Filter @{AwsAccountId =
 [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =
 "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =
 "EQUALS"; Value = 'FAILED'}}
```

> **Note**
>
> `CompanyName` 또는 `ProductName` 기준으로 조사 결과를 필터링하면 Security Hub CSPM은 `ProductFields` ASFF 객체에 있는 값을 사용합니다. Security Hub CSPM은 최상위 `CompanyName` 및 `ProductName` 필드를 사용하지 않습니다.

## Security Hub CSPM에서 조사 결과 필터링

AWS Security Hub CSPM은 보안 검사에서 자체 결과를 생성하고 통합 제품에서 결과를 수신합니다. Security Hub CSPM 콘솔의 조사 결과, 통합 및 인사이트 페이지에서 조사 결과 목록을 표시할 수 있습니다. 조사 결과 목록이 조직 또는 사용 사례와 관련성이 높도록 필터를 추가하여 목록의 범위를 좁힐 수 있습니다.

특정 보안 제어에 대한 조사 결과를 필터링하는 방법에 대한 자세한 내용은 the section called “제어 조사 결과 필터링 및 정렬” 섹션을 참조하세요. 이 페이지의 정보는 조사 결과, 인사이트 및 통합 페이지에 적용됩니다.

## 조사 결과 목록의 기본 필터

기본적으로 Security Hub CSPM 콘솔의 조사 결과 목록은 AWS Security Finding Format(ASFF)의 `RecordState` 및 `Workflow.Status` 필드를 기준으로 필터링됩니다. 이는 특정 인사이트 또는 통합을 위한 필터에 추가됩니다.

기록 상태는 조사 결과가 활성 상태인지 보관 상태인지 여부를 나타냅니다. 기본적으로 조사 결과 목록에는 활성 조사 결과만 표시됩니다. 조사 결과 공급자는 더 이상 활성 상태가 아니거나 중요하지 않은 조사 결과를 보관할 수 있습니다. 또한 Security Hub CSPM은 연결된 리소스가 삭제되면 제어 조사 결과를 자동으로 보관합니다.

워크플로 상태는 조사 결과에 대한 조사 상태를 나타냅니다. 기본적으로 조사 결과 목록에는 워크플로 상태가 `NEW` 또는 `NOTIFIED`인 조사 결과만 표시됩니다. 조사 결과의 워크플로 상태를 업데이트할 수 있습니다.

## 필터 추가 지침

조사 결과 목록을 최대 10개의 속성으로 필터링할 수 있습니다. 각 속성에 대해 최대 20개의 필터 값을 입력할 수 있습니다.

조사 결과 목록을 필터링할 때 Security Hub CSPM은 필터 집합에 `AND` 논리를 적용합니다. 조사 결과는 제공된 모든 필터와 일치해야 합니다. 예를 들어, GuardDuty를 제품 이름의 필터로 추가하고 `AwsS3Bucket`을 리소스 유형의 필터로 추가하는 경우, Security Hub CSPM은 두 기준 모두와 일치하는 조사 결과를 표시합니다.

Security Hub CSPM은 동일한 속성이지만 다른 값을 사용하는 필터에 `OR` 로직을 적용합니다. 예를 들어 GuardDuty와 Amazon Inspector를 모두 제품 이름의 필터 값으로 추가하면 Security Hub CSPM은 GuardDuty 또는 Amazon Inspector에서 생성된 조사 결과를 표시합니다.

조사 결과 목록에 필터를 추가하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 조사 결과 목록을 표시하려면 탐색 창에서 다음 작업 중 하나를 수행합니다.
    - 조사 결과를 선택합니다.

- 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.
- [통합(Integrations)]을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.

3. 필터 추가 상자에서 필터링 기준으로 사용할 필드를 하나 이상 선택합니다.

   회사 이름 또는 제품 이름을 기준으로 필터링하면 콘솔은 AWS Security Finding 형식(ASFF)의 최상위 `CompanyName` 및 `ProductName` 필드를 사용합니다. API는 `ProductFields` 아래에 중첩된 값을 사용합니다.

4. 필터 일치 유형을 선택합니다.

   문자열 필터의 경우, 다음 옵션 중에서 선택할 수 있습니다.

   - is - 필터 값과 정확히 일치하는 값을 찾습니다.
   - starts with - 필터 값으로 시작하는 값을 찾습니다.
   - is not - 필터 값과 일치하지 않는 값을 찾습니다.
   - does not start with - 필터 값으로 시작하지 않는 값을 찾습니다.

   리소스 태그 필드의 경우 특정 키 또는 값을 기준으로 필터링할 수 있습니다.

   숫자 필터의 경우, 단일 숫자(단일) 또는 숫자 범위(범위) 중에서 어느 것을 입력할지 선택할 수 있습니다.

   날짜 또는 시간 필터의 경우, 현재 날짜 시간(롤링 윈도우) 또는 날짜 범위(고정 범위) 중 어느 기간을 입력할지 선택할 수 있습니다.

   필터를 여러 개 추가하면 다음과 같은 상호 작용이 발생합니다.

   - is 및 with start 필터는 OR로 조인됩니다. 필터 값이 하나라도 포함되어 있으면 값이 일치합니다. 예를 들어, 심각도 레이블을 중요로 지정하고 심각도 레이블을 높음으로 지정하면 결과에는 심각도 중요 및 심각도 높음 조사 결과가 모두 포함됩니다.
   - is not 및 does not start with 필터는 AND로 조인됩니다. 값은 해당 필터 값을 포함하지 않는 경우에만 일치합니다. 예를 들어, 심각도 레이블이 낮지 않음으로 지정하고 심각도 레이블이 중간이 아님으로 지정한 경우, 조사 결과에는 심각도 낮음 또는 심각도 중간 조사 결과가 포함되지 않습니다.

   필드에 is 필터가 있는 경우, 동일한 필드에서 is not 또는 does not start with 필터를 가질 수 없습니다.

5. 필터 값을 지정합니다. 문자열 필터의 경우, 필터 값은 대/소문자를 구분합니다.
6. 적용을 선택합니다.

   기존 필터의 경우, 필터 일치 유형 또는 값을 변경할 수 있습니다. 필터링된 조사 결과 목록에서 필터를 선택합니다. 필터 편집 상자에서 새로운 일치 유형 또는 값을 선택한 다음 적용을 선택합니다.

   필터를 제거하려면 x 아이콘을 선택합니다. 목록이 자동으로 업데이트되어 변경 사항을 반영합니다.

## Security Hub CSPM에서 조사 결과 그룹화

AWS Security Hub CSPM에서 선택한 속성의 값을 기준으로 조사 결과를 그룹화할 수 있습니다.

조사 결과를 그룹화하면 조사 결과 목록이 일치하는 조사 결과에서 선택한 속성의 값 목록으로 바뀝니다. 각 값의 경우, 목록에는 일치하는 조사 결과의 수가 표시됩니다.

예를 들어 조사 결과를 AWS 계정 ID별로 그룹화하면 계정 식별자 목록과 각 계정의 일치하는 조사 결과 수가 표시됩니다.

Security Hub CSPM은 선택한 속성에 대해 최대 100개의 값을 표시할 수 있습니다. 값이 100개를 초과하는 경우, 처음 100개만 표시됩니다.

속성 값을 선택하면 Security Hub CSPM이 해당 값과 일치하는 조사 결과의 목록을 표시합니다.

조사 결과 목록에서 조사 결과를 그룹화하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 조사 결과 목록을 표시하려면 탐색 창에서 다음 작업 중 하나를 수행합니다.

   - 조사 결과를 선택합니다.
   - 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.
   - [통합(Integrations)]을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.
3. 그룹화 드롭다운에서 그룹화에 사용할 속성을 선택합니다.

   그룹화 속성을 제거하려면 x 아이콘을 선택합니다. 그룹화 속성을 제거하면 목록이 속성 값 목록에서 조사 결과 목록으로 변경됩니다.

# Security Hub CSPM에서 조사 결과의 워크플로 상태 설정

워크플로 상태는 조사 결과에 대한 조사 진행 상황을 추적합니다. 워크플로 상태는 개별 조사 결과에 고유하며 새 조사 결과의 생성에는 영향을 미치지 않습니다. 예를 들어, 조사 결과의 워크플로 상태를 SUPPRESSED 또는 RESOLVED로 설정해도 Security Hub CSPM이 동일한 문제에 대한 새로운 조사 결과를 생성하는 것을 방지할 수 없습니다.

조사 결과의 워크플로 상태는 다음 값 중 하나일 수 있습니다.

신규

검토하기 전 조사 결과의 초기 상태입니다.

AWS 서비스와 같이 통합된에서 수집된 결과는 초기 상태로 NEW를 AWS Config갖습니다.

또한 Security Hub CSPM은 다음과 같은 경우, 워크플로 상태를 NOTIFIED 또는 RESOLVED에서 NEW로 재설정합니다.

- RecordState은(는) ARCHIVED에서 ACTIVE(으)로 바뀝니다.
- Compliance.Status은(는) PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE(으)로 바뀝니다.

이러한 변경은 추가 조사가 필요하다는 것을 의미합니다.

알림

리소스 소유자에게 보안 문제에 대해 통지했음을 나타냅니다. 리소스 소유자가 아닌 경우, 이 상태를 사용할 수 있으며 보안 문제를 해결하기 위해 리소스 소유자의 개입이 필요합니다.

다음 중 하나가 발생하면 워크플로우 상태가 자동으로 NOTIFIED에서 NEW으(로) 변경됩니다.

- RecordState은(는) ARCHIVED에서 ACTIVE(으)로 바뀝니다.
- Compliance.Status은(는) PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE(으)로 바뀝니다.

억제됨

결과를 검토한 조사 결과 조치가 필요하지 않다고 생각함을 나타냅니다.

RecordState이(가) ARCHIVED에서 ACTIVE(으)로 변경되더라도 SUPPRESSED 조사 결과의 워크플로 상태는 변경되지 않습니다.

해결됨

조사 결과가 검토 및 수정되었으며 이제 해결된 것으로 간주됩니다.

다음 중 하나가 발생하지 않는 한 조사 결과는 RESOLVED로 유지됩니다.

- RecordState은(는) ARCHIVED에서 ACTIVE(으)로 바뀝니다.
- Compliance.Status은(는) PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE(으)로 바뀝니다.

이 경우, 워크플로 상태는 자동으로 NEW로 재설정됩니다.

제어 조사 결과의 경우, Compliance.Status가 PASSED이면 Security Hub CSPM은 자동으로 워크플로 상태를 RESOLVED으로 설정합니다.

## 조사 결과에 대한 워크플로 상태 설정

하나 이상의 조사 결과의 워크플로 상태를 변경하려면 Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용할 수 있습니다. 조사 결과의 워크플로 상태를 변경하는 경우 Security Hub CSPM이 요청을 처리하고 조사 결과를 업데이트하는 데 몇 분 정도 걸릴 수 있습니다.

> **Tip**
>
> 자동화 규칙을 사용하여 조사 결과의 워크플로 상태를 자동으로 변경할 수도 있습니다. 자동화 규칙을 사용하면 지정한 기준에 따라 조사 결과의 워크플로 상태를 자동으로 업데이트하도록 Security Hub CSPM을 구성할 수 있습니다. 자세한 내용은 Security Hub CSPM의 자동화 규칙 이해 단원을 참조하십시오.

하나 이상의 조사 결과의 워크플로 상태를 변경하려면 원하는 방법을 선택하고 단계를 수행합니다.

Security Hub CSPM console

조사 결과의 워크플로 상태를 변경하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 다음 중 하나를 수행하여 조사 결과 테이블을 표시합니다.
   - 조사 결과를 선택합니다.

- 인사이트를 선택합니다. 그런 다음 인사이트를 선택합니다. 인사이트 결과에서 결과를 선택합니다.
- [통합(Integrations)]을 선택합니다. 그런 다음 통합 섹션에서 조사 결과 보기를 선택합니다.
- 보안 표준을 선택합니다. 그런 다음 표준 섹션에서 결과 보기를 선택합니다. 제어 테이블에서 제어를 선택하여 해당 제어에 대한 조사 결과를 표시합니다.

3. 조사 결과 테이블에서 워크플로 상태를 변경하려는 각 조사 결과의 확인란을 선택합니다.
4. 페이지 상단에서 워크플로 상태를 선택한 다음 선택한 조사 결과의 새 워크플로 상태를 선택합니다.
5. 워크플로 상태 설정 대화 상자에서 선택적으로 워크플로 상태 변경 이유를 자세히 설명하는 메모를 입력합니다. 그런 다음 상태 설정을 선택합니다.

Security Hub CSPM API

BatchUpdateFindings 작업을 사용합니다. 조사 결과 ID 및 조사 결과를 생성했던 제품의 ARN을 모두 입력합니다. GetFindings 작업을 사용하여 이러한 세부 정보를 가져올 수 있습니다.

AWS CLI

batch-update-findings 명령을 실행합니다. 조사 결과 ID 및 조사 결과를 생성했던 제품의 ARN을 모두 입력합니다. get-findings 명령을 실행하여 이러한 세부 정보를 가져올 수 있습니다.

```
batch-update-findings --finding-identifiers
 Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

예제

```
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"
```

## 사용자 지정 Security Hub CSPM 작업으로 조사 결과 전송

AWS Security Hub CSPM 사용자 지정 작업을 생성하여 Amazon EventBridge로 Security Hub CSPM을 자동화할 수 있습니다. 사용자 지정 작업의 경우, 이벤트 유형은 Security Hub Findings - Custom Action입니다. 사용자 지정 작업을 설정한 후 조사 결과를 해당 작업에 전송할 수 있습니다. 사용자 지

정 작업을 만드는 방법에 대한 자세한 내용과 단계는 the section called “자동 응답 및 해결” 섹션을 참조하세요.

조사 결과를 사용자 지정 작업으로 전송하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 조사 결과 목록을 표시하려면 다음 중 하나를 수행하세요.
   - Security Hub CSPM 탐색 창에서 조사 결과를 선택합니다.
   - Security Hub CSPM 탐색 창에서 인사이트를 선택합니다. 인사이트를 선택합니다. 그런 다음 결과 목록에서 인사이트 결과를 선택합니다.
   - Security Hub CSPM 탐색 창에서 통합을 선택합니다. 통합에 대해 조사 결과 보기를 선택합니다.
   - Security Hub CSPM 탐색 창에서 보안 표준을 선택합니다. 결과 보기를 선택하여 제어 목록을 표시합니다. 그런 다음 제어 이름을 선택합니다.
3. 조사 결과 목록에서 사용자 지정 작업으로 전송할 각 조사 결과의 확인란을 선택합니다.

   조사 결과를 한 번에 최대 20개까지 선택할 수 있습니다.
4. 작업에서 사용자 지정 작업을 선택합니다.

## AWS 보안 조사 결과 형식(ASFF)

AWS Security Hub CSPM은 통합 및 타사 제품의 결과를 소비 AWS 서비스 하고 집계합니다. Security Hub CSPM은 AWS Security Finding Format(ASFF)이라는 표준 조사 결과 형식을 사용하여 이러한 조사 결과를 처리하므로 시간이 많이 걸리는 데이터 변환 작업이 필요하지 않습니다.

이 페이지에서는 AWS Security Finding Format(ASFF)의 조사 결과에 대한 JSON의 전체 개요를 제공합니다. 이 형식은 JSON 스키마에서 파생됩니다. 연결된 객체의 이름을 선택하면 해당 객체에 대한 예시 조사 결과를 검토할 수 있습니다. Security Hub CSPM 조사 결과를 여기에 표시된 리소스 및 예시와 비교하면 조사 결과를 해석하는 데 도움이 될 수 있습니다.

개별 ASFF 속성에 대한 설명은 the section called “필수 최상위 ASFF 속성” 및 the section called “선택적 최상위 ASFF 속성” 섹션을 참조하세요.

```
"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"
     }
]
```

# ASFF 필드 및 값에 대한 통합의 영향

AWS Security Hub CSPM은 제어를 위한 두 가지 유형의 통합을 제공합니다.

- 통합 제어 보기 - 이 유형의 통합을 통해 각 제어는 모든 표준에서 단일 식별자가 지정됩니다. 또한 Security Hub CSPM 콘솔의 제어 페이지에는 모든 표준의 모든 제어가 표시됩니다.
- 통합 제어 조사 결과 - 이 유형의 통합을 통해 Security Hub CSPM은 제어가 여러 활성화된 표준에 적용되더라도 해당 제어에 대한 단일 조사 결과를 생성합니다. 이렇게 하면 조사 결과 노이즈를 줄일 수 있습니다.

통합 제어 보기는 활성화하거나 비활성화할 수 없습니다. 2023년 2월 23일 이후에 Security Hub CSPM을 활성화하면 통합 제어 조사 결과가 기본적으로 활성화됩니다. 그렇지 않으면 기본적으로 비활성화됩니다. 그러나 조직의 경우 통합 제어 조사 결과는 Security Hub CSPM이 관리자 계정에서 활성화된 경우에만 Security Hub CSPM 멤버 계정에서 활성화됩니다. 통합 제어 결과에 대한 자세한 내용은 제어 조사 결과 생성 및 업데이트 섹션을 참조하세요.

두 유형의 통합 모두 AWS 보안 조사 결과 형식(ASFF)의 제어 조사 결과에 대한 필드 및 값에 영향을 미칩니다.

주제

- 통합 제어 보기 - ASFF 변경
- 통합 제어 조사 결과 - ASFF 변경
- 통합 제어 조사 결과를 활성화하기 전 및 후의 생성기 ID
- 통합이 제어 ID 및 제목에 미치는 영향
- 통합을 위한 워크플로 업데이트

## 통합 제어 보기 - ASFF 변경

통합 제어 보기 기능으로 인해 ASFF의 제어 조사 결과 필드 및 값이 다음과 같이 변경되었습니다. 워크플로가 이러한 ASFF 필드의 값을 사용하지 않는 경우, 조치가 필요하지 않습니다. 이러한 필드의 특정 값에 의존하는 워크플로가 있는 경우, 현재 값을 사용하도록 워크플로를 업데이트하세요.

| ASFF 필드 | 통합 제어 보기 이전의 샘플 값 | 통합 제어 보기 이후의 샘플 값 및 변경 내용 설명 |
| --- | --- | --- |
| Compliance.SecurityControlId | 해당 없음 (새로운 필드) | EC2.2 |

| ASFF 필드 | 통합 제어 보기 이전의 샘플 값 | 통합 제어 보기 이후의 샘플 값 및 변경 내용 설명 |
| --- | --- | --- |
| | | 표준 전체에 단일 제어 ID를 도입합니다. `ProductFields.RuleId` 은(는) 여전히 CIS v1.2.0 제어에 대한 표준 기반 제어 ID를 제공합니다. `ProductFields.ControlId` 은(는) 다른 표준의 제어에 대해 여전히 표준 기반 제어 ID를 제공합니다. |
| Compliance.AssociatedStandards | 해당 없음 (새로운 필드) | [{"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"}]<br><br>제어가 활성화된 표준을 보여줍니다. |
| ProductFields.ArchivalReasons:0/Description | 해당 없음 (새로운 필드) | “통합 제어 조사 결과가 켜져 있거나 꺼졌기 때문에 조사 결과는 ARCHIVED 상태입니다. 이로 인해 새로운 조사 결과가 생성될 때 이전 상태의 조사 결과가 보관됩니다.”<br><br>Security Hub CSPM이 기존 조사 결과를 보관한 이유를 설명합니다. |
| ProductFields.ArchivalReasons:0/ReasonCode | 해당 없음 (새로운 필드) | "CONSOLIDATED_CONTROL_FINDINGS_UPDATE"<br><br>Security Hub CSPM이 기존 조사 결과를 보관한 이유를 제공합니다. |

| ASFF 필드 | 통합 제어 보기 이전의 샘플 값 | 통합 제어 보기 이후의 샘플 값 및 변경 내용 설명 |
|---|---|---|
| ProductFields.RecommendationUrl | https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation | https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |
| Remediation.Recommendation.Text | “이 문제를 해결하는 방법에 대한 지침은 AWS Security Hub CSPM PCI DSS 설명서를 참조하세요.” | “이 문제를 해결하는 방법에 대한 지침은 AWS Security Hub CSPM 제어 설명서를 참조하세요.”<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |
| Remediation.Recommendation.Url | https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation | https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |

통합 제어 조사 결과 - ASFF 변경

통합 제어 조사 결과를 활성화하면 ASFF의 제어 조사 결과 필드 및 값이 다음과 같이 변경될 수 있습니다. 이러한 변경 사항은 통합 제어 보기 기능에 의해 도입된 변경 사항에 추가됩니다. 워크플로가 이러한 ASFF 필드의 값을 사용하지 않는 경우, 조치가 필요하지 않습니다. 이러한 필드의 특정 값에 의존하는 워크플로가 있는 경우, 현재 값을 사용하도록 워크플로를 업데이트하세요.

> **Tip**
>
> AWS v2.0.0에서 자동 보안 대응 솔루션을 사용하는 경우 통합 제어 조사 결과를 지원한다는 점에 유의하세요. 즉, 통합 제어 조사 결과를 활성화하면 현재 워크플로를 유지할 수 있습니다.

| ASFF 필드 | 통합 제어 조사 결과를 활성화하기 이전의 샘플 값 | 통합 제어 조사 결과를 활성화한 이후의 샘플 값 및 변경 내용 설명 |
|---|---|---|
| GeneratorId | aws-foundational-security-best-practices/v/1.0.0/Config.1 | security-control/Config.1<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |
| 제목 | PCI.Config.1을 활성화해야 AWS Config 합니다. | AWS Config 를 활성화해야 합니다.<br><br>이 필드는 더 이상 표준별 정보를 참조하지 않습니다. |
| Id | arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.IAM.5/finding/ab6d6a26-a156-48f0-9403-115983e5a956 | arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |
| ProductFields.ControlId | PCI.EC2.2 | 제거되었습니다. 대신 `Compliance.SecurityControlId` 섹션을 참조하세요.<br><br>이 필드는 표준에 구애받지 않는 단일 제어 ID를 위해 제거되었습니다. |
| ProductFields.RuleID | 1.3 | 제거되었습니다. 대신 `Compliance.SecurityControlId` 섹션을 참조하세요.<br><br>이 필드는 표준에 구애받지 않는 단일 제어 ID를 위해 제거되었습니다. |

| ASFF 필드 | 통합 제어 조사 결과를 활성화하기 이전의 샘플 값 | 통합 제어 조사 결과를 활성화한 이후의 샘플 값 및 변경 내용 설명 |
|---|---|---|
| 설명 | 이 PCI DSS 제어 AWS Config 는 현재 계정 및 리전에서가 활성화되어 있는지 확인합니다. | 이 AWS 제어 AWS Config 는 현재 계정 및 리전에서가 활성화되어 있는지 확인합니다.<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |
| 심각도 | "Severity": {<br><br>"Product": 90,<br><br>"Label": "CRITICAL",<br><br>"Normalized": 90,<br><br>"Original": "CRITICAL"<br><br>} | "Severity": {<br><br>"Label": "CRITICAL",<br><br>"Normalized": 90,<br><br>"Original": "CRITICAL"<br><br>}<br><br>Security Hub CSPM은 조사 결과의 심각도를 설명하기 위해 더 이상 제품 필드를 사용하지 않습니다. |
| 유형 | ["Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"] | ["Software and Configuration Checks/Industry and Regulatory Standards"]<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |

| ASFF 필드 | 통합 제어 조사 결과를 활성화하기 이전의 샘플 값 | 통합 제어 조사 결과를 활성화한 이후의 샘플 값 및 변경 내용 설명 |
|---|---|---|
| Compliance.Related Requirements | ["PCI DSS 10.5.2",<br>"PCI DSS 11.5",<br>"CIS AWS 파운데이션 2.5"] | ["PCI DSS v3.2.1/10.5.2",<br>“PCI DSS v3.2.1/11.5",<br>"CIS AWS 파운데이션 벤치마크 v1.2.0/2.5"]<br>이 필드에는 활성화된 모든 표준의 관련 요구 사항이 표시됩니다. |
| CreatedAt | 2022-05-05T08:18:13.138Z | 2022-09-25T08:18:13.138Z<br>형식은 동일하게 유지되지만 통합 제어 조사 결과를 활성화하면 값이 재설정됩니다. |
| FirstObservedAt | 2022-05-07T08:18:13.138Z | 2022-09-28T08:18:13.138Z<br>형식은 동일하게 유지되지만 통합 제어 조사 결과를 활성화하면 값이 재설정됩니다. |
| ProductFields.RecommendationUrl | https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation | 제거되었습니다. 대신 `Remediation.Recommendation.Url` 섹션을 참조하세요. |
| ProductFields.StandardsArn | arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0 | 제거되었습니다. 대신 `Compliance.AssociatedStandards` 섹션을 참조하세요. |
| ProductFields.StandardsControlArn | arn:aws:securityhub:us-east-1:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/Config.1 | 제거되었습니다. Security Hub CSPM은 표준 전반에 걸쳐 보안 검사에 대한 하나의 조사 결과를 생성합니다. |

| ASFF 필드 | 통합 제어 조사 결과를 활성화하기 이전의 샘플 값 | 통합 제어 조사 결과를 활성화한 이후의 샘플 값 및 변경 내용 설명 |
|---|---|---|
| ProductFields.StandardsGuideArn | arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0 | 제거되었습니다. 대신 `Compliance.AssociatedStandards` 섹션을 참조하세요. |
| ProductFields.StandardsGuideSubscriptionArn | arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0 | 제거되었습니다. Security Hub CSPM은 표준 전반에 걸쳐 보안 검사에 대한 하나의 조사 결과를 생성합니다. |
| ProductFields.StandardsSubscriptionArn | arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0 | 제거되었습니다. Security Hub CSPM은 표준 전반에 걸쳐 보안 검사에 대한 하나의 조사 결과를 생성합니다. |
| ProductFields.aws/securityhub/FindingId | arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 | arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/Config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67<br><br>이 필드는 더 이상 표준을 참조하지 않습니다. |

통합 제어 조사 결과를 켠 후 고객이 입력한 ASFF 필드의 새 값

통합 제어 조사 결과를 활성화하면 Security Hub CSPM은 표준 전반에 걸쳐 하나의 조사 결과를 생성하고 원래 조사 결과(각 표준에 대한 별도의 조사 결과)를 보관합니다.

Security Hub CSPM 콘솔 또는 BatchUpdateFindings 작업을 사용하여 원래 조사 결과를 업데이트한 내용은 새 조사 결과에 보존되지 않습니다. 필요한 경우 보관된 조사 결과를 참조하여 이 데이터를 복구할 수 있습니다. 보관된 조사 결과를 검토하려면 Security Hub CSPM 콘솔의 조사 결과 페이

지를 사용하여 레코드 상태 필터를 보관됨으로 설정할 수 있습니다. 또는 Security Hub CSPM API의 GetFindings 작업을 사용할 수 있습니다.

| 고객이 입력한 ASFF 필드 | 통합 제어 조사 결과를 활성화한 이후의 변경 내용 설명 |
|---|---|
| 신뢰도 | 빈 상태로 재설정합니다. |
| 중요도 | 빈 상태로 재설정합니다. |
| 참고 | 빈 상태로 재설정합니다. |
| RelatedFindings | 빈 상태로 재설정합니다. |
| 심각도 | 조사 결과의 기본 심각도(제어의 심각도와 일치) |
| 유형 | 표준에 구애받지 않는 값으로 재설정합니다. |
| UserDefinedFields | 빈 상태로 재설정합니다. |
| VerificationState | 빈 상태로 재설정합니다. |
| 워크플로 | 실패한 새로운 조사 결과의 기본값은 NEW입니다. 전달된 새로운 조사 결과의 기본값은 RESOLVED입니다. |

통합 제어 조사 결과를 활성화하기 전 및 후의 생성기 ID

다음 표에는 통합 제어 조사 결과를 활성화할 때 제어의 생성기 ID 값에 대한 변경 사항이 나열되어 있습니다. 이러한 변경 사항은 2023년 2월 15일 현재 Security Hub CSPM이 지원하는 제어에 적용됩니다.

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.1 | security-control/CloudWatch.1 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.10 | security-control/IAM.16 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.11 | security-control/IAM.17 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.12 | security-control/IAM.4 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.13 | security-control/IAM.9 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.14 | security-control/IAM.6 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.16 | security-control/IAM.2 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.2 | security-control/IAM.5 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.20 | security-control/IAM.18 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.22 | security-control/IAM.1 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.3 | security-control/IAM.8 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.4 | security-control/IAM.3 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.5 | security-control/IAM.11 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.6 | security-control/IAM.12 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.7 | security-control/IAM.13 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.8 | security-control/IAM.14 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/1.9 | security-control/IAM.15 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.1 | security-control/CloudTrail.1 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.2 | security-control/CloudTrail.4 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.3 | security-control/CloudTrail.6 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.4 | security-control/CloudTrail.5 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.5 | security-control/Config.1 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.6 | security-control/CloudTrail.7 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.7 | security-control/CloudTrail.2 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.8 | security-control/KMS.4 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/2.9 | security-control/EC2.6 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.1 | security-control/CloudWatch.2 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.2 | security-control/CloudWatch.3 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.3 | security-control/CloudWatch.1 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.4 | security-control/CloudWatch.4 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.5 | security-control/CloudWatch.5 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.6 | security-control/CloudWatch.6 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.7 | security-control/CloudWatch.7 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.8 | security-control/CloudWatch.8 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.9 | security-control/CloudWatch.9 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.10 | security-control/CloudWatch.10 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.11 | security-control/CloudWatch.11 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.12 | security-control/CloudWatch.12 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.13 | security-control/CloudWatch.13 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/3.14 | security-control/CloudWatch.14 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.1 | security-control/EC2.13 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.2 | security-control/EC2.14 |
| arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule/4.3 | security-control/EC2.2 |
| cis-aws-foundations-benchmark/v/1.4.0/1.10 | security-control/IAM.5 |
| cis-aws-foundations-benchmark/v/1.4.0/1.14 | security-control/IAM.3 |
| cis-aws-foundations-benchmark/v/1.4.0/1.16 | security-control/IAM.1 |
| cis-aws-foundations-benchmark/v/1.4.0/1.17 | security-control/IAM.18 |
| cis-aws-foundations-benchmark/v/1.4.0/1.4 | security-control/IAM.4 |
| cis-aws-foundations-benchmark/v/1.4.0/1.5 | security-control/IAM.9 |
| cis-aws-foundations-benchmark/v/1.4.0/1.6 | security-control/IAM.6 |
| cis-aws-foundations-benchmark/v/1.4.0/1.7 | security-control/CloudWatch.1 |
| cis-aws-foundations-benchmark/v/1.4.0/1.8 | security-control/IAM.15 |
| cis-aws-foundations-benchmark/v/1.4.0/1.9 | security-control/IAM.16 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| cis-aws-foundations-benchmark/v/1.4.0/2.1.2 | security-control/S3.5 |
| cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1 | security-control/S3.1 |
| cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2 | security-control/S3.8 |
| cis-aws-foundations-benchmark/v/1.4.0/2.2.1 | security-control/EC2.7 |
| cis-aws-foundations-benchmark/v/1.4.0/2.3.1 | security-control/RDS.3 |
| cis-aws-foundations-benchmark/v/1.4.0/3.1 | security-control/CloudTrail.1 |
| cis-aws-foundations-benchmark/v/1.4.0/3.2 | security-control/CloudTrail.4 |
| cis-aws-foundations-benchmark/v/1.4.0/3.4 | security-control/CloudTrail.5 |
| cis-aws-foundations-benchmark/v/1.4.0/3.5 | security-control/Config.1 |
| cis-aws-foundations-benchmark/v/1.4.0/3.6 | security-control/S3.9 |
| cis-aws-foundations-benchmark/v/1.4.0/3.7 | security-control/CloudTrail.2 |
| cis-aws-foundations-benchmark/v/1.4.0/3.8 | security-control/KMS.4 |
| cis-aws-foundations-benchmark/v/1.4.0/3.9 | security-control/EC2.6 |
| cis-aws-foundations-benchmark/v/1.4.0/4.3 | security-control/CloudWatch.1 |
| cis-aws-foundations-benchmark/v/1.4.0/4.4 | security-control/CloudWatch.4 |
| cis-aws-foundations-benchmark/v/1.4.0/4.5 | security-control/CloudWatch.5 |
| cis-aws-foundations-benchmark/v/1.4.0/4.6 | security-control/CloudWatch.6 |
| cis-aws-foundations-benchmark/v/1.4.0/4.7 | security-control/CloudWatch.7 |
| cis-aws-foundations-benchmark/v/1.4.0/4.8 | security-control/CloudWatch.8 |
| cis-aws-foundations-benchmark/v/1.4.0/4.9 | security-control/CloudWatch.9 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| cis-aws-foundations-benchmark/v/1.4.0/4.10 | security-control/CloudWatch.10 |
| cis-aws-foundations-benchmark/v/1.4.0/4.11 | security-control/CloudWatch.11 |
| cis-aws-foundations-benchmark/v/1.4.0/4.12 | security-control/CloudWatch.12 |
| cis-aws-foundations-benchmark/v/1.4.0/4.13 | security-control/CloudWatch.13 |
| cis-aws-foundations-benchmark/v/1.4.0/4.14 | security-control/CloudWatch.14 |
| cis-aws-foundations-benchmark/v/1.4.0/5.1 | security-control/EC2.21 |
| cis-aws-foundations-benchmark/v/1.4.0/5.3 | security-control/EC2.2 |
| aws-foundational-security-best-practices/v/1.0.0/Account.1 | security-control/Account.1 |
| aws-foundational-security-best-practices/v/1.0.0/ACM.1 | security-control/ACM.1 |
| aws-foundational-security-best-practices/v/1.0.0/APIGateway.1 | security-control/APIGateway.1 |
| aws-foundational-security-best-practices/v/1.0.0/APIGateway.2 | security-control/APIGateway.2 |
| aws-foundational-security-best-practices/v/1.0.0/APIGateway.3 | security-control/APIGateway.3 |
| aws-foundational-security-best-practices/v/1.0.0/APIGateway.4 | security-control/APIGateway.4 |
| aws-foundational-security-best-practices/v/1.0.0/APIGateway.5 | security-control/APIGateway.5 |
| aws-foundational-security-best-practices/v/1.0.0/APIGateway.8 | security-control/APIGateway.8 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| aws-foundational-security-best-practices/v/1.0.0/APIGateway.9 | security-control/APIGateway.9 |
| aws-foundational-security-best-practices/v/1.0.0/AutoScaling.1 | security-control/AutoScaling.1 |
| aws-foundational-security-best-practices/v/1.0.0/AutoScaling.2 | security-control/AutoScaling.2 |
| aws-foundational-security-best-practices/v/1.0.0/AutoScaling.3 | security-control/AutoScaling.3 |
| aws-foundational-security-best-practices/v/1.0.0/Autoscaling.5 | security-control/Autoscaling.5 |
| aws-foundational-security-best-practices/v/1.0.0/AutoScaling.6 | security-control/AutoScaling.6 |
| aws-foundational-security-best-practices/v/1.0.0/AutoScaling.9 | security-control/AutoScaling.9 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.1 | security-control/CloudFront.1 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.3 | security-control/CloudFront.3 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.4 | security-control/CloudFront.4 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.5 | security-control/CloudFront.5 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.6 | security-control/CloudFront.6 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.7 | security-control/CloudFront.7 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.8 | security-control/CloudFront.8 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.9 | security-control/CloudFront.9 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.10 | security-control/CloudFront.10 |
| aws-foundational-security-best-practices/v/1.0.0/CloudFront.12 | security-control/CloudFront.12 |
| aws-foundational-security-best-practices/v/1.0.0/CloudTrail.1 | security-control/CloudTrail.1 |
| aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2 | security-control/CloudTrail.2 |
| aws-foundational-security-best-practices/v/1.0.0/CloudTrail.4 | security-control/CloudTrail.4 |
| aws-foundational-security-best-practices/v/1.0.0/CloudTrail.5 | security-control/CloudTrail.5 |
| aws-foundational-security-best-practices/v/1.0.0/CodeBuild.1 | security-control/CodeBuild.1 |
| aws-foundational-security-best-practices/v/1.0.0/CodeBuild.2 | security-control/CodeBuild.2 |
| aws-foundational-security-best-practices/v/1.0.0/CodeBuild.3 | security-control/CodeBuild.3 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/CodeBuild.4 | security-control/CodeBuild.4 |
| aws-foundational-security-best-practices/v/1.0.0/Config.1 | security-control/Config.1 |
| aws-foundational-security-best-practices/v/1.0.0/DMS.1 | security-control/DMS.1 |
| aws-foundational-security-best-practices/v/1.0.0/DynamoDB.1 | security-control/DynamoDB.1 |
| aws-foundational-security-best-practices/v/1.0.0/DynamoDB.2 | security-control/DynamoDB.2 |
| aws-foundational-security-best-practices/v/1.0.0/DynamoDB.3 | security-control/DynamoDB.3 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.1 | security-control/EC2.1 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.3 | security-control/EC2.3 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.4 | security-control/EC2.4 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.6 | security-control/EC2.6 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.7 | security-control/EC2.7 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.8 | security-control/EC2.8 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| aws-foundational-security-best-practices/v/1.0.0/EC2.9 | security-control/EC2.9 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.10 | security-control/EC2.10 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.15 | security-control/EC2.15 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.16 | security-control/EC2.16 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.17 | security-control/EC2.17 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.18 | security-control/EC2.18 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.19 | security-control/EC2.19 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.2 | security-control/EC2.2 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.20 | security-control/EC2.20 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.21 | security-control/EC2.21 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.23 | security-control/EC2.23 |
| aws-foundational-security-best-practices/v/1.0.0/EC2.24 | security-control/EC2.24 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| aws-foundational-security-best-practices/v/1.0.0/EC2.25 | security-control/EC2.25 |
| aws-foundational-security-best-practices/v/1.0.0/ECR.1 | security-control/ECR.1 |
| aws-foundational-security-best-practices/v/1.0.0/ECR.2 | security-control/ECR.2 |
| aws-foundational-security-best-practices/v/1.0.0/ECR.3 | security-control/ECR.3 |
| aws-foundational-security-best-practices/v/1.0.0/ECS.10 | security-control/ECS.10 |
| aws-foundational-security-best-practices/v/1.0.0/ECS.12 | security-control/ECS.12 |
| aws-foundational-security-best-practices/v/1.0.0/ECS.2 | security-control/ECS.2 |
| aws-foundational-security-best-practices/v/1.0.0/ECS.3 | security-control/ECS.3 |
| aws-foundational-security-best-practices/v/1.0.0/ECS.4 | security-control/ECS.4 |
| aws-foundational-security-best-practices/v/1.0.0/ECS.5 | security-control/ECS.5 |
| aws-foundational-security-best-practices/v/1.0.0/ECS.8 | security-control/ECS.8 |
| aws-foundational-security-best-practices/v/1.0.0/EFS.1 | security-control/EFS.1 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/EFS.2 | security-control/EFS.2 |
| aws-foundational-security-best-practices/v/1.0.0/EFS.3 | security-control/EFS.3 |
| aws-foundational-security-best-practices/v/1.0.0/EFS.4 | security-control/EFS.4 |
| aws-foundational-security-best-practices/v/1.0.0/EKS.2 | security-control/EKS.2 |
| aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.1 | security-control/ElasticBeanstalk.1 |
| aws-foundational-security-best-practices/v/1.0.0/ElasticBeanstalk.2 | security-control/ElasticBeanstalk.2 |
| aws-foundational-security-best-practices/v/1.0.0/ELBv2.1 | security-control/ELB.1 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.2 | security-control/ELB.2 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.3 | security-control/ELB.3 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.4 | security-control/ELB.4 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.5 | security-control/ELB.5 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.6 | security-control/ELB.6 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/ELB.7 | security-control/ELB.7 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.8 | security-control/ELB.8 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.9 | security-control/ELB.9 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.10 | security-control/ELB.10 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.11 | security-control/ELB.11 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.12 | security-control/ELB.12 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.13 | security-control/ELB.13 |
| aws-foundational-security-best-practices/v/1.0.0/ELB.14 | security-control/ELB.14 |
| aws-foundational-security-best-practices/v/1.0.0/EMR.1 | security-control/EMR.1 |
| aws-foundational-security-best-practices/v/1.0.0/ES.1 | security-control/ES.1 |
| aws-foundational-security-best-practices/v/1.0.0/ES.2 | security-control/ES.2 |
| aws-foundational-security-best-practices/v/1.0.0/ES.3 | security-control/ES.3 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/ES.4 | security-control/ES.4 |
| aws-foundational-security-best-practices/v/1.0.0/ES.5 | security-control/ES.5 |
| aws-foundational-security-best-practices/v/1.0.0/ES.6 | security-control/ES.6 |
| aws-foundational-security-best-practices/v/1.0.0/ES.7 | security-control/ES.7 |
| aws-foundational-security-best-practices/v/1.0.0/ES.8 | security-control/ES.8 |
| aws-foundational-security-best-practices/v/1.0.0/GuardDuty.1 | security-control/GuardDuty.1 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.1 | security-control/IAM.1 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.2 | security-control/IAM.2 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.21 | security-control/IAM.21 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.3 | security-control/IAM.3 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.4 | security-control/IAM.4 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.5 | security-control/IAM.5 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/IAM.6 | security-control/IAM.6 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.7 | security-control/IAM.7 |
| aws-foundational-security-best-practices/v/1.0.0/IAM.8 | security-control/IAM.8 |
| aws-foundational-security-best-practices/v/1.0.0/Kinesis.1 | security-control/Kinesis.1 |
| aws-foundational-security-best-practices/v/1.0.0/KMS.1 | security-control/KMS.1 |
| aws-foundational-security-best-practices/v/1.0.0/KMS.2 | security-control/KMS.2 |
| aws-foundational-security-best-practices/v/1.0.0/KMS.3 | security-control/KMS.3 |
| aws-foundational-security-best-practices/v/1.0.0/Lambda.1 | security-control/Lambda.1 |
| aws-foundational-security-best-practices/v/1.0.0/Lambda.2 | security-control/Lambda.2 |
| aws-foundational-security-best-practices/v/1.0.0/Lambda.5 | security-control/Lambda.5 |
| aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.3 | security-control/NetworkFirewall.3 |
| aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.4 | security-control/NetworkFirewall.4 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.5 | security-control/NetworkFirewall.5 |
| aws-foundational-security-best-practices/v/1.0.0/NetworkFirewall.6 | security-control/NetworkFirewall.6 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.1 | security-control/Opensearch.1 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.2 | security-control/Opensearch.2 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.3 | security-control/Opensearch.3 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.4 | security-control/Opensearch.4 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.5 | security-control/Opensearch.5 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.6 | security-control/Opensearch.6 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.7 | security-control/Opensearch.7 |
| aws-foundational-security-best-practices/v/1.0.0/Opensearch.8 | security-control/Opensearch.8 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.1 | security-control/RDS.1 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.10 | security-control/RDS.10 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| aws-foundational-security-best-practices/v/1.0.0/RDS.11 | security-control/RDS.11 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.12 | security-control/RDS.12 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.13 | security-control/RDS.13 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.14 | security-control/RDS.14 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.15 | security-control/RDS.15 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.16 | security-control/RDS.16 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.17 | security-control/RDS.17 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.19 | security-control/RDS.19 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.2 | security-control/RDS.2 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.20 | security-control/RDS.20 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.21 | security-control/RDS.21 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.22 | security-control/RDS.22 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/RDS.23 | security-control/RDS.23 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.24 | security-control/RDS.24 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.25 | security-control/RDS.25 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.3 | security-control/RDS.3 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.4 | security-control/RDS.4 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.5 | security-control/RDS.5 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.6 | security-control/RDS.6 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.7 | security-control/RDS.7 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.8 | security-control/RDS.8 |
| aws-foundational-security-best-practices/v/1.0.0/RDS.9 | security-control/RDS.9 |
| aws-foundational-security-best-practices/v/1.0.0/Redshift.1 | security-control/Redshift.1 |
| aws-foundational-security-best-practices/v/1.0.0/Redshift.2 | security-control/Redshift.2 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/Redshift.3 | security-control/Redshift.3 |
| aws-foundational-security-best-practices/v/1.0.0/Redshift.4 | security-control/Redshift.4 |
| aws-foundational-security-best-practices/v/1.0.0/Redshift.6 | security-control/Redshift.6 |
| aws-foundational-security-best-practices/v/1.0.0/Redshift.7 | security-control/Redshift.7 |
| aws-foundational-security-best-practices/v/1.0.0/Redshift.8 | security-control/Redshift.8 |
| aws-foundational-security-best-practices/v/1.0.0/S3.1 | security-control/S3.1 |
| aws-foundational-security-best-practices/v/1.0.0/S3.12 | security-control/S3.12 |
| aws-foundational-security-best-practices/v/1.0.0/S3.13 | security-control/S3.13 |
| aws-foundational-security-best-practices/v/1.0.0/S3.2 | security-control/S3.2 |
| aws-foundational-security-best-practices/v/1.0.0/S3.3 | security-control/S3.3 |
| aws-foundational-security-best-practices/v/1.0.0/S3.5 | security-control/S3.5 |
| aws-foundational-security-best-practices/v/1.0.0/S3.6 | security-control/S3.6 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/S3.8 | security-control/S3.8 |
| aws-foundational-security-best-practices/v/1.0.0/S3.9 | security-control/S3.9 |
| aws-foundational-security-best-practices/v/1.0.0/SageMaker.1 | security-control/SageMaker.1 |
| aws-foundational-security-best-practices/v/1.0.0/SageMaker.2 | security-control/SageMaker.2 |
| aws-foundational-security-best-practices/v/1.0.0/SageMaker.3 | security-control/SageMaker.3 |
| aws-foundational-security-best-practices/v/1.0.0/SecretsManager.1 | security-control/SecretsManager.1 |
| aws-foundational-security-best-practices/v/1.0.0/SecretsManager.2 | security-control/SecretsManager.2 |
| aws-foundational-security-best-practices/v/1.0.0/SecretsManager.3 | security-control/SecretsManager.3 |
| aws-foundational-security-best-practices/v/1.0.0/SecretsManager.4 | security-control/SecretsManager.4 |
| aws-foundational-security-best-practices/v/1.0.0/SQS.1 | security-control/SQS.1 |
| aws-foundational-security-best-practices/v/1.0.0/SSM.1 | security-control/SSM.1 |
| aws-foundational-security-best-practices/v/1.0.0/SSM.2 | security-control/SSM.2 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| aws-foundational-security-best-practices/v/1.0.0/SSM.3 | security-control/SSM.3 |
| aws-foundational-security-best-practices/v/1.0.0/SSM.4 | security-control/SSM.4 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.1 | security-control/WAF.1 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.2 | security-control/WAF.2 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.3 | security-control/WAF.3 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.4 | security-control/WAF.4 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.6 | security-control/WAF.6 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.7 | security-control/WAF.7 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.8 | security-control/WAF.8 |
| aws-foundational-security-best-practices/v/1.0.0/WAF.10 | security-control/WAF.10 |
| pci-dss/v/3.2.1/PCI.AutoScaling.1 | security-control/AutoScaling.1 |
| pci-dss/v/3.2.1/PCI.CloudTrail.1 | security-control/CloudTrail.2 |
| pci-dss/v/3.2.1/PCI.CloudTrail.2 | security-control/CloudTrail.3 |
| pci-dss/v/3.2.1/PCI.CloudTrail.3 | security-control/CloudTrail.4 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| pci-dss/v/3.2.1/PCI.CloudTrail.4 | security-control/CloudTrail.5 |
| pci-dss/v/3.2.1/PCI.CodeBuild.1 | security-control/CodeBuild.1 |
| pci-dss/v/3.2.1/PCI.CodeBuild.2 | security-control/CodeBuild.2 |
| pci-dss/v/3.2.1/PCI.Config.1 | security-control/Config.1 |
| pci-dss/v/3.2.1/PCI.CW.1 | security-control/CloudWatch.1 |
| pci-dss/v/3.2.1/PCI.DMS.1 | security-control/DMS.1 |
| pci-dss/v/3.2.1/PCI.EC2.1 | security-control/EC2.1 |
| pci-dss/v/3.2.1/PCI.EC2.2 | security-control/EC2.2 |
| pci-dss/v/3.2.1/PCI.EC2.4 | security-control/EC2.12 |
| pci-dss/v/3.2.1/PCI.EC2.5 | security-control/EC2.13 |
| pci-dss/v/3.2.1/PCI.EC2.6 | security-control/EC2.6 |
| pci-dss/v/3.2.1/PCI.ELBv2.1 | security-control/ELB.1 |
| pci-dss/v/3.2.1/PCI.ES.1 | security-control/ES.2 |
| pci-dss/v/3.2.1/PCI.ES.2 | security-control/ES.1 |
| pci-dss/v/3.2.1/PCI.GuardDuty.1 | security-control/GuardDuty.1 |
| pci-dss/v/3.2.1/PCI.IAM.1 | security-control/IAM.4 |
| pci-dss/v/3.2.1/PCI.IAM.2 | security-control/IAM.2 |
| pci-dss/v/3.2.1/PCI.IAM.3 | security-control/IAM.1 |
| pci-dss/v/3.2.1/PCI.IAM.4 | security-control/IAM.6 |
| pci-dss/v/3.2.1/PCI.IAM.5 | security-control/IAM.9 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| pci-dss/v/3.2.1/PCI.IAM.6 | security-control/IAM.19 |
| pci-dss/v/3.2.1/PCI.IAM.7 | security-control/IAM.8 |
| pci-dss/v/3.2.1/PCI.IAM.8 | security-control/IAM.10 |
| pci-dss/v/3.2.1/PCI.KMS.1 | security-control/KMS.4 |
| pci-dss/v/3.2.1/PCI.Lambda.1 | security-control/Lambda.1 |
| pci-dss/v/3.2.1/PCI.Lambda.2 | security-control/Lambda.3 |
| pci-dss/v/3.2.1/PCI.Opensearch.1 | security-control/Opensearch.2 |
| pci-dss/v/3.2.1/PCI.Opensearch.2 | security-control/Opensearch.1 |
| pci-dss/v/3.2.1/PCI.RDS.1 | security-control/RDS.1 |
| pci-dss/v/3.2.1/PCI.RDS.2 | security-control/RDS.2 |
| pci-dss/v/3.2.1/PCI.Redshift.1 | security-control/Redshift.1 |
| pci-dss/v/3.2.1/PCI.S3.1 | security-control/S3.3 |
| pci-dss/v/3.2.1/PCI.S3.2 | security-control/S3.2 |
| pci-dss/v/3.2.1/PCI.S3.3 | security-control/S3.7 |
| pci-dss/v/3.2.1/PCI.S3.5 | security-control/S3.5 |
| pci-dss/v/3.2.1/PCI.S3.6 | security-control/S3.1 |
| pci-dss/v/3.2.1/PCI.SageMaker.1 | security-control/SageMaker.1 |
| pci-dss/v/3.2.1/PCI.SSM.1 | security-control/SSM.2 |
| pci-dss/v/3.2.1/PCI.SSM.2 | security-control/SSM.3 |
| pci-dss/v/3.2.1/PCI.SSM.3 | security-control/SSM.1 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| service-managed-aws-control-tower/v/1.0.0/ACM.1 | security-control/ACM.1 |
| service-managed-aws-control-tower/v/1.0.0/APIGateway.1 | security-control/APIGateway.1 |
| service-managed-aws-control-tower/v/1.0.0/APIGateway.2 | security-control/APIGateway.2 |
| service-managed-aws-control-tower/v/1.0.0/APIGateway.3 | security-control/APIGateway.3 |
| service-managed-aws-control-tower/v/1.0.0/APIGateway.4 | security-control/APIGateway.4 |
| service-managed-aws-control-tower/v/1.0.0/APIGateway.5 | security-control/APIGateway.5 |
| service-managed-aws-control-tower/v/1.0.0/AutoScaling.1 | security-control/AutoScaling.1 |
| service-managed-aws-control-tower/v/1.0.0/AutoScaling.2 | security-control/AutoScaling.2 |
| service-managed-aws-control-tower/v/1.0.0/AutoScaling.3 | security-control/AutoScaling.3 |
| service-managed-aws-control-tower/v/1.0.0/AutoScaling.4 | security-control/AutoScaling.4 |
| service-managed-aws-control-tower/v/1.0.0/Autoscaling.5 | security-control/Autoscaling.5 |
| service-managed-aws-control-tower/v/1.0.0/AutoScaling.6 | security-control/AutoScaling.6 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| service-managed-aws-control-tower/v/1.0.0/AutoScaling.9 | security-control/AutoScaling.9 |
| service-managed-aws-control-tower/v/1.0.0/CloudTrail.1 | security-control/CloudTrail.1 |
| service-managed-aws-control-tower/v/1.0.0/CloudTrail.2 | security-control/CloudTrail.2 |
| service-managed-aws-control-tower/v/1.0.0/CloudTrail.4 | security-control/CloudTrail.4 |
| service-managed-aws-control-tower/v/1.0.0/CloudTrail.5 | security-control/CloudTrail.5 |
| service-managed-aws-control-tower/v/1.0.0/CodeBuild.1 | security-control/CodeBuild.1 |
| service-managed-aws-control-tower/v/1.0.0/CodeBuild.2 | security-control/CodeBuild.2 |
| service-managed-aws-control-tower/v/1.0.0/CodeBuild.4 | security-control/CodeBuild.4 |
| service-managed-aws-control-tower/v/1.0.0/CodeBuild.5 | security-control/CodeBuild.5 |
| service-managed-aws-control-tower/v/1.0.0/DMS.1 | security-control/DMS.1 |
| service-managed-aws-control-tower/v/1.0.0/DynamoDB.1 | security-control/DynamoDB.1 |
| service-managed-aws-control-tower/v/1.0.0/DynamoDB.2 | security-control/DynamoDB.2 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/EC2.1 | security-control/EC2.1 |
| service-managed-aws-control-tower/v/1.0.0/EC2.2 | security-control/EC2.2 |
| service-managed-aws-control-tower/v/1.0.0/EC2.3 | security-control/EC2.3 |
| service-managed-aws-control-tower/v/1.0.0/EC2.4 | security-control/EC2.4 |
| service-managed-aws-control-tower/v/1.0.0/EC2.6 | security-control/EC2.6 |
| service-managed-aws-control-tower/v/1.0.0/EC2.7 | security-control/EC2.7 |
| service-managed-aws-control-tower/v/1.0.0/EC2.8 | security-control/EC2.8 |
| service-managed-aws-control-tower/v/1.0.0/EC2.9 | security-control/EC2.9 |
| service-managed-aws-control-tower/v/1.0.0/EC2.10 | security-control/EC2.10 |
| service-managed-aws-control-tower/v/1.0.0/EC2.15 | security-control/EC2.15 |
| service-managed-aws-control-tower/v/1.0.0/EC2.16 | security-control/EC2.16 |
| service-managed-aws-control-tower/v/1.0.0/EC2.17 | security-control/EC2.17 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/EC2.18 | security-control/EC2.18 |
| service-managed-aws-control-tower/v/1.0.0/EC2.19 | security-control/EC2.19 |
| service-managed-aws-control-tower/v/1.0.0/EC2.20 | security-control/EC2.20 |
| service-managed-aws-control-tower/v/1.0.0/EC2.21 | security-control/EC2.21 |
| service-managed-aws-control-tower/v/1.0.0/EC2.22 | security-control/EC2.22 |
| service-managed-aws-control-tower/v/1.0.0/ECR.1 | security-control/ECR.1 |
| service-managed-aws-control-tower/v/1.0.0/ECR.2 | security-control/ECR.2 |
| service-managed-aws-control-tower/v/1.0.0/ECR.3 | security-control/ECR.3 |
| service-managed-aws-control-tower/v/1.0.0/ECS.2 | security-control/ECS.2 |
| service-managed-aws-control-tower/v/1.0.0/ECS.3 | security-control/ECS.3 |
| service-managed-aws-control-tower/v/1.0.0/ECS.4 | security-control/ECS.4 |
| service-managed-aws-control-tower/v/1.0.0/ECS.5 | security-control/ECS.5 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/ECS.8 | security-control/ECS.8 |
| service-managed-aws-control-tower/v/1.0.0/ECS.10 | security-control/ECS.10 |
| service-managed-aws-control-tower/v/1.0.0/ECS.12 | security-control/ECS.12 |
| service-managed-aws-control-tower/v/1.0.0/EFS.1 | security-control/EFS.1 |
| service-managed-aws-control-tower/v/1.0.0/EFS.2 | security-control/EFS.2 |
| service-managed-aws-control-tower/v/1.0.0/EFS.3 | security-control/EFS.3 |
| service-managed-aws-control-tower/v/1.0.0/EFS.4 | security-control/EFS.4 |
| service-managed-aws-control-tower/v/1.0.0/EKS.2 | security-control/EKS.2 |
| service-managed-aws-control-tower/v/1.0.0/ELB.2 | security-control/ELB.2 |
| service-managed-aws-control-tower/v/1.0.0/ELB.3 | security-control/ELB.3 |
| service-managed-aws-control-tower/v/1.0.0/ELB.4 | security-control/ELB.4 |
| service-managed-aws-control-tower/v/1.0.0/ELB.5 | security-control/ELB.5 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/ELB.6 | security-control/ELB.6 |
| service-managed-aws-control-tower/v/1.0.0/ELB.7 | security-control/ELB.7 |
| service-managed-aws-control-tower/v/1.0.0/ELB.8 | security-control/ELB.8 |
| service-managed-aws-control-tower/v/1.0.0/ELB.9 | security-control/ELB.9 |
| service-managed-aws-control-tower/v/1.0.0/ELB.10 | security-control/ELB.10 |
| service-managed-aws-control-tower/v/1.0.0/ELB.12 | security-control/ELB.12 |
| service-managed-aws-control-tower/v/1.0.0/ELB.13 | security-control/ELB.13 |
| service-managed-aws-control-tower/v/1.0.0/ELB.14 | security-control/ELB.14 |
| service-managed-aws-control-tower/v/1.0.0/ELBv2.1 | security-control/ELBv2.1 |
| service-managed-aws-control-tower/v/1.0.0/EMR.1 | security-control/EMR.1 |
| service-managed-aws-control-tower/v/1.0.0/ES.1 | security-control/ES.1 |
| service-managed-aws-control-tower/v/1.0.0/ES.2 | security-control/ES.2 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/ES.3 | security-control/ES.3 |
| service-managed-aws-control-tower/v/1.0.0/ES.4 | security-control/ES.4 |
| service-managed-aws-control-tower/v/1.0.0/ES.5 | security-control/ES.5 |
| service-managed-aws-control-tower/v/1.0.0/ES.6 | security-control/ES.6 |
| service-managed-aws-control-tower/v/1.0.0/ES.7 | security-control/ES.7 |
| service-managed-aws-control-tower/v/1.0.0/ES.8 | security-control/ES.8 |
| service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.1 | security-control/ElasticBeanstalk.1 |
| service-managed-aws-control-tower/v/1.0.0/ElasticBeanstalk.2 | security-control/ElasticBeanstalk.2 |
| service-managed-aws-control-tower/v/1.0.0/GuardDuty.1 | security-control/GuardDuty.1 |
| service-managed-aws-control-tower/v/1.0.0/IAM.1 | security-control/IAM.1 |
| service-managed-aws-control-tower/v/1.0.0/IAM.2 | security-control/IAM.2 |
| service-managed-aws-control-tower/v/1.0.0/IAM.3 | security-control/IAM.3 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/IAM.4 | security-control/IAM.4 |
| service-managed-aws-control-tower/v/1.0.0/IAM.5 | security-control/IAM.5 |
| service-managed-aws-control-tower/v/1.0.0/IAM.6 | security-control/IAM.6 |
| service-managed-aws-control-tower/v/1.0.0/IAM.7 | security-control/IAM.7 |
| service-managed-aws-control-tower/v/1.0.0/IAM.8 | security-control/IAM.8 |
| service-managed-aws-control-tower/v/1.0.0/IAM.21 | security-control/IAM.21 |
| service-managed-aws-control-tower/v/1.0.0/Kinesis.1 | security-control/Kinesis.1 |
| service-managed-aws-control-tower/v/1.0.0/KMS.1 | security-control/KMS.1 |
| service-managed-aws-control-tower/v/1.0.0/KMS.2 | security-control/KMS.2 |
| service-managed-aws-control-tower/v/1.0.0/KMS.3 | security-control/KMS.3 |
| service-managed-aws-control-tower/v/1.0.0/Lambda.1 | security-control/Lambda.1 |
| service-managed-aws-control-tower/v/1.0.0/Lambda.2 | security-control/Lambda.2 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| service-managed-aws-control-tower/v/1.0.0/Lambda.5 | security-control/Lambda.5 |
| service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.3 | security-control/NetworkFirewall.3 |
| service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.4 | security-control/NetworkFirewall.4 |
| service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.5 | security-control/NetworkFirewall.5 |
| service-managed-aws-control-tower/v/1.0.0/NetworkFirewall.6 | security-control/NetworkFirewall.6 |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.1 | security-control/Opensearch.1 |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.2 | security-control/Opensearch.2 |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.3 | security-control/Opensearch.3 |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.4 | security-control/Opensearch.4 |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.5 | security-control/Opensearch.5 |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.6 | security-control/Opensearch.6 |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.7 | security-control/Opensearch.7 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/Opensearch.8 | security-control/Opensearch.8 |
| service-managed-aws-control-tower/v/1.0.0/RDS.1 | security-control/RDS.1 |
| service-managed-aws-control-tower/v/1.0.0/RDS.2 | security-control/RDS.2 |
| service-managed-aws-control-tower/v/1.0.0/RDS.3 | security-control/RDS.3 |
| service-managed-aws-control-tower/v/1.0.0/RDS.4 | security-control/RDS.4 |
| service-managed-aws-control-tower/v/1.0.0/RDS.5 | security-control/RDS.5 |
| service-managed-aws-control-tower/v/1.0.0/RDS.6 | security-control/RDS.6 |
| service-managed-aws-control-tower/v/1.0.0/RDS.8 | security-control/RDS.8 |
| service-managed-aws-control-tower/v/1.0.0/RDS.9 | security-control/RDS.9 |
| service-managed-aws-control-tower/v/1.0.0/RDS.10 | security-control/RDS.10 |
| service-managed-aws-control-tower/v/1.0.0/RDS.11 | security-control/RDS.11 |
| service-managed-aws-control-tower/v/1.0.0/RDS.13 | security-control/RDS.13 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/RDS.17 | security-control/RDS.17 |
| service-managed-aws-control-tower/v/1.0.0/RDS.19 | security-control/RDS.19 |
| service-managed-aws-control-tower/v/1.0.0/RDS.20 | security-control/RDS.20 |
| service-managed-aws-control-tower/v/1.0.0/RDS.21 | security-control/RDS.21 |
| service-managed-aws-control-tower/v/1.0.0/RDS.22 | security-control/RDS.22 |
| service-managed-aws-control-tower/v/1.0.0/RDS.23 | security-control/RDS.23 |
| service-managed-aws-control-tower/v/1.0.0/RDS.25 | security-control/RDS.25 |
| service-managed-aws-control-tower/v/1.0.0/Redshift.1 | security-control/Redshift.1 |
| service-managed-aws-control-tower/v/1.0.0/Redshift.2 | security-control/Redshift.2 |
| service-managed-aws-control-tower/v/1.0.0/Redshift.4 | security-control/Redshift.4 |
| service-managed-aws-control-tower/v/1.0.0/Redshift.6 | security-control/Redshift.6 |
| service-managed-aws-control-tower/v/1.0.0/Redshift.7 | security-control/Redshift.7 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
|---|---|
| service-managed-aws-control-tower/v/1.0.0/Redshift.8 | security-control/Redshift.8 |
| service-managed-aws-control-tower/v/1.0.0/S3.1 | security-control/S3.1 |
| service-managed-aws-control-tower/v/1.0.0/S3.2 | security-control/S3.2 |
| service-managed-aws-control-tower/v/1.0.0/S3.3 | security-control/S3.3 |
| service-managed-aws-control-tower/v/1.0.0/S3.5 | security-control/S3.5 |
| service-managed-aws-control-tower/v/1.0.0/S3.6 | security-control/S3.6 |
| service-managed-aws-control-tower/v/1.0.0/S3.8 | security-control/S3.8 |
| service-managed-aws-control-tower/v/1.0.0/S3.9 | security-control/S3.9 |
| service-managed-aws-control-tower/v/1.0.0/S3.12 | security-control/S3.12 |
| service-managed-aws-control-tower/v/1.0.0/S3.13 | security-control/S3.13 |
| service-managed-aws-control-tower/v/1.0.0/SageMaker.1 | security-control/SageMaker.1 |
| service-managed-aws-control-tower/v/1.0.0/SecretsManager.1 | security-control/SecretsManager.1 |

| 통합 제어 조사 결과를 활성화하기 이전의 GeneratorID | 통합 제어 조사 결과를 활성화한 이후의 GeneratorID |
| --- | --- |
| service-managed-aws-control-tower/v/1.0.0/SecretsManager.2 | security-control/SecretsManager.2 |
| service-managed-aws-control-tower/v/1.0.0/SecretsManager.3 | security-control/SecretsManager.3 |
| service-managed-aws-control-tower/v/1.0.0/SecretsManager.4 | security-control/SecretsManager.4 |
| service-managed-aws-control-tower/v/1.0.0/SQS.1 | security-control/SQS.1 |
| service-managed-aws-control-tower/v/1.0.0/SSM.1 | security-control/SSM.1 |
| service-managed-aws-control-tower/v/1.0.0/SSM.2 | security-control/SSM.2 |
| service-managed-aws-control-tower/v/1.0.0/SSM.3 | security-control/SSM.3 |
| service-managed-aws-control-tower/v/1.0.0/SSM.4 | security-control/SSM.4 |
| service-managed-aws-control-tower/v/1.0.0/WAF.2 | security-control/WAF.2 |
| service-managed-aws-control-tower/v/1.0.0/WAF.3 | security-control/WAF.3 |
| service-managed-aws-control-tower/v/1.0.0/WAF.4 | security-control/WAF.4 |

### 통합이 제어 ID 및 제목에 미치는 영향

통합 제어 보기 및 통합 제어 조사 결과는 표준 전반에 걸쳐 제어 ID 및 제목을 표준화합니다. 보안 제어 ID 및 보안 제어 제목이라는 용어는 이러한 표준에 구애받지 않는 값을 나타냅니다.

Security Hub CSPM 콘솔에는 사용자의 계정에서 통합 제어 조사 결과가 활성화되어 있는지 여부에 관계없이 보안 제어 ID 및 보안 제어 제목이 표시됩니다. 그러나, 사용자의 계정에서 통합 제어 조사 결과가 비활성화된 경우, Security Hub CSPM 조사 결과에는 표준별 제어 제목(PCI 및 CIS v1.2.0용)이 포함됩니다. 또한 Security Hub CSPM 조사 결과에는 표준별 제어 ID 및 보안 제어 ID가 포함됩니다. 통합이 제어 조사 결과에 미치는 영향의 예는 제어 조사 결과 샘플 섹션을 참조하세요.

AWS Control Tower 서비스 관리형 표준에 속하는 제어의 경우, 통합 제어 조사 결과가 활성화되면 조사 결과의 제어 ID 및 제목에서 접두사 `CT.`가 제거됩니다.

Security Hub CSPM에서 보안 제어를 비활성화하려면 보안 제어에 해당하는 모든 표준 제어를 비활성화해야 합니다. 다음 테이블은 보안 제어 ID 및 제목과 표준별 제어 ID 및 제목의 매핑을 보여줍니다. AWS 기본 보안 모범 사례(FSBP) 표준에 속하는 제어의 IDs 및 제목은 이미 표준에 구애받지 않습니다. 인터넷 보안 센터(CIS) v3.0.0의 요구 사항에 대한 제어 매핑은 각 버전의 CIS 요구 사항에 대한 제어 매핑 섹션을 참조하세요. 이 테이블에 스크립트를 직접 실행하려면 스크립트를 .csv 파일로 다운로드할 수 있습니다.

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.2.0 | 1.1 루트 사용자의 사용을 피합니다. | [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다. |
| CIS v1.2.0 | 1.10 IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다. | [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다. |
| CIS v1.2.0 | 1.11 IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다. | [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다. |
| CIS v1.2.0 | 1.12 루트 사용자 액세스 키가 없는지 여부를 확인합니다. | [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다. |
| CIS v1.2.0 | 1.13 루트 사용자에 대해 MFA가 활성화되어 있는지 여부를 확인합니다. | [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.2.0 | 1.14 루트 사용자에 대해 하드웨어 MFA가 활성화되어 있는지 여부를 확인합니다. | [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다. |
| CIS v1.2.0 | 1.16 IAM 정책이 그룹 또는 역할에만 연결되어 있는지 여부를 확인합니다. | [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다. |
| CIS v1.2.0 | 1.2 콘솔 암호가 있는 모든 IAM 사용자에 대해 다중 인증(MFA)이 활성화되었는지 여부를 확인합니다. | [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다. |
| CIS v1.2.0 | 1.20 지원을(를) 통해 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인합니다 | [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support |
| CIS v1.2.0 | 1.22 전체 '*:*' 관리 권한을 허용하는 IAM 정책이 생성되지 않았는지 확인합니다. | [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다. |
| CIS v1.2.0 | 1.3 90일 이상 사용하지 않은 자격 증명이 비활성화되어 있는지 여부를 확인합니다. | [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다. |
| CIS v1.2.0 | 1.4 90일이 되기 전에 액세스 키가 교체되는지 여부를 확인합니다. | [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다. |
| CIS v1.2.0 | 1.5 IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다. | [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다. |
| CIS v1.2.0 | 1.6 IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다. | [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다. |
| CIS v1.2.0 | 1.7 IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다. | [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.2.0 | 1.8 IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다. | [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다. |
| CIS v1.2.0 | 1.9 IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다. | [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다. |
| CIS v1.2.0 | 2.1 모든 리전에서 CloudTrail이 활성화되어 있는지 여부를 확인합니다. | [CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다. |
| CIS v1.2.0 | 2.2 CloudTrail 로그 파일 검증이 활성화되어 있는지 여부를 확인합니다. | [CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다. |
| CIS v1.2.0 | 2.3 CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인합니다. | [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요. |
| CIS v1.2.0 | 2.4 CloudTrail 추적이 CloudWatch Logs와 통합되었는지 확인합니다. | [CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. |
| CIS v1.2.0 | 2.5 AWS Config 가 활성화되어 있는지 확인 | [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. |
| CIS v1.2.0 | 2.6 CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다. | [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다. |
| CIS v1.2.0 | 2.7 KMS CMK를 사용하여 CloudTrail 로그가 저장 시 암호화되는지 확인합니다. | [CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다. |
| CIS v1.2.0 | 2.8 고객이 생성한 CMK에 대한 교체가 활성화되었는지 확인합니다. | [KMS.4]AWS KMS키 교체를 활성화해야 합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.2.0 | 2.9 모든 VPC에서 VPC 흐름 로깅이 활성화되어 있는지 확인합니다. | [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다. |
| CIS v1.2.0 | 3.1 무단 API 직접 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.2] 무단 API 호출에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.10 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.11 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.12 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.13 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.14 VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.2 MFA 없는 로그인에 대해 관리 콘솔에 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.3] MFA 없는 로그인에 대해 관리 콘솔에 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.3 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다. | [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.2.0 | 3.4 IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.5 CloudTrail 구성 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다 |
| CIS v1.2.0 | 3.6 AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | [CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인 |
| CIS v1.2.0 | 3.7 고객 생성 CMK 활성화 또는 예약된 삭제에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다. |
| CIS v1.2.0 | 3.8 S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.2.0 | 3.9 AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | [CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인 |
| CIS v1.2.0 | 4.1 어떤 보안 그룹에서도 0.0.0.0/0에서 포트 22로의 수신을 허용하지 않는지 여부를 확인합니다. | [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다. |
| CIS v1.2.0 | 4.2 어떤 보안 그룹에서도 0.0.0.0/0에서 포트 3389로의 수신을 허용하지 않는지 여부를 확인합니다. | [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다. |
| CIS v1.2.0 | 4.3 모든 VPC의 기본 보안 그룹이 모든 트래픽을 제한하는지 여부를 확인합니다. | [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.4.0 | 1.10 콘솔 암호가 있는 모든 IAM 사용자에 대해 다중 인증(MFA)이 활성화되었는지 여부를 확인합니다. | [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다. |
| CIS v1.4.0 | 1.4 90일이 되기 전에 액세스 키가 교체되는지 여부를 확인합니다. | [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다. |
| CIS v1.4.0 | 1.16 전체 '*:*' 관리 권한을 허용하는 IAM 정책이 연결되지 않았는지 확인합니다. | [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다. |
| CIS v1.4.0 | 1.17 지원을(를) 통해 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인합니다 | [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support |
| CIS v1.4.0 | 1.4 루트 사용자 계정 액세스 키가 없는지 여부를 확인합니다. | [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다. |
| CIS v1.4.0 | 1.5 루트 사용자 계정에 대해 MFA가 활성화되어 있는지 확인합니다. | [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다. |
| CIS v1.4.0 | 1.6 루트 사용자 계정에 대해 하드웨어 MFA가 활성화되어 있는지 확인합니다. | [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다. |
| CIS v1.4.0 | 1.7 관리 및 일상 작업에 루트 사용자 사용을 제거합니다. | [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다. |
| CIS v1.4.0 | 1.8 IAM 비밀번호 정책에서 14자 이상을 요구하는지 여부를 확인합니다. | [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다. |
| CIS v1.4.0 | 1.9 IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다. | [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.4.0 | 2.1.2 S3 버킷 정책이 HTTP 요청을 거부하도록 설정되어 있는지 확인합니다. | [S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다. |
| CIS v1.4.0 | 2.1.5.1 S3 퍼블릭 액세스 차단 설정을 활성화해야 합니다. | [S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다 |
| CIS v1.4.0 | 2.1.5.2 S3 퍼블릭 액세스 차단 설정은 버킷 수준에서 활성화되어야 합니다. | [S3.8] S3 범용 버킷은 퍼블릭 액세스를 차단해야 합니다. |
| CIS v1.4.0 | 2.2.1 EBS 볼륨 암호화가 활성화되었는지 확인합니다. | [EC2.7] EBS 기본 암호화를 활성화해야 합니다. |
| CIS v1.4.0 | 2.3.1 RDS 인스턴스에 암호화가 활성화되어 있는지 확인합니다. | [RDS.3] RDS DB 인스턴스에는 저장 데이터 암호화가 활성화되어 있어야 합니다. |
| CIS v1.4.0 | 3.1 모든 리전에서 CloudTrail이 활성화되어 있는지 여부를 확인합니다. | [CloudTrail.1] CloudTrail은 읽기 및 쓰기 관리 이벤트를 포함하는 하나 이상의 다중 리전 추적으로 활성화되고 구성되어야 합니다. |
| CIS v1.4.0 | 3.2 CloudTrail 로그 파일 검증이 활성화되어 있는지 여부를 확인합니다. | [CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다. |
| CIS v1.4.0 | 3.4 CloudTrail 추적이 CloudWatch Logs와 통합되었는지 확인합니다. | [CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. |
| CIS v1.4.0 | 3.5 모든 리전에서 AWS Config 가 활성화되어 있는지 확인 | [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. |
| CIS v1.4.0 | 3.6 CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다. | [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
| --- | --- | --- |
| CIS v1.4.0 | 3.7 KMS CMK를 사용하여 CloudTrail 로그가 저장 시 암호화되는지 확인합니다. | [CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다. |
| CIS v1.4.0 | 3.8 고객이 생성한 CMK에 대한 교체가 활성화되었는지 확인합니다. | [KMS.4]AWS KMS키 교체를 활성화해야 합니다. |
| CIS v1.4.0 | 3.9 모든 VPC에서 VPC 흐름 로깅이 활성화되어 있는지 확인합니다. | [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다. |
| CIS v1.4.0 | 4.4 IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.4] IAM 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.4.0 | 4.5 CloudTrail 구성 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.5] CloudTrail 구성 변경에 대한 로그 지표 필터 및 경보가 있는지 확인합니다 |
| CIS v1.4.0 | 4.6 AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | [CloudWatch.6] AWS Management Console 인증 실패에 대한 로그 지표 필터 및 경보가 존재하는지 확인 |
| CIS v1.4.0 | 4.7 고객 생성 CMK 활성화 또는 예약된 삭제에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.7] 고객 관리 키의 비활성화 또는 예약 삭제에 대한 로그 메트릭 필터 및 경보가 있는지 확인합니다. |
| CIS v1.4.0 | 4.8 S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.8] S3 버킷 정책 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.4.0 | 4.9 AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인 | [CloudWatch.9] AWS Config 구성 변경에 대한 로그 지표 필터 및 경보가 존재하는지 확인 |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| CIS v1.4.0 | 4.10 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.10] 보안 그룹 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.4.0 | 4.11 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.11] 네트워크 액세스 제어 목록(NACL) 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.4.0 | 4.12 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.12] 네트워크 게이트웨이 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.4.0 | 4.13 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.13] 라우팅 테이블 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.4.0 | 4.14 VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. | [CloudWatch.14] VPC 변경 사항에 대해 로그 메트릭 필터 및 경보가 존재하는지 여부를 확인합니다. |
| CIS v1.4.0 | 5.1 네트워크 ACL이 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않는지 확인합니다. | [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다. |
| CIS v1.4.0 | 5.3 모든 VPC의 기본 보안 그룹이 모든 트래픽을 제한하는지 여부를 확인합니다. | [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다. |
| PCI DSS v3.2.1 | PCI.AutoScaling.1 로드 밸런서와 연결된 Auto Scaling 그룹은 로드 밸런서 상태 확인을 사용해야 합니다. | [PCI.AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다. |
| PCI DSS v3.2.1 | PCI.CloudTrail.1 CloudTrail 로그는 AWS KMS CMKs | [CloudTrail.2] CloudTrail에서 유휴 시 암호화를 활성화해야 합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| PCI DSS v3.2.1 | PCI.CloudTrail.2 CloudTrail을 활성화해야 합니다. | [CloudTrail.3] 하나 이상의 CloudTrail 추적을 활성화해야 합니다. |
| PCI DSS v3.2.1 | PCI.CloudTrail.3 CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다. | [CloudTrail.4] CloudTrail 로그 파일 유효성 검증을 활성화해야 합니다. |
| PCI DSS v3.2.1 | PCI.CloudTrail.4 CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. | [CloudTrail.5] CloudTrail 추적은 Amazon CloudWatch Logs와 통합되어야 합니다. |
| PCI DSS v3.2.1 | PCI CodeBuild GitHub 또는 Bitbucket 소스 리포지토리 URL은 OAuth를 사용해야 합니다. | [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다. |
| PCI DSS v3.2.1 | PCI.CodeBuild.2 CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다. | [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다. |
| PCI DSS v3.2.1 | PCI.Config.1을 활성화해야 AWS Config 합니다. | [Config.1]를 활성화하고 리소스 기록을 위해 서비스 연결 역할을 사용해야 AWS Config 합니다. |
| PCI DSS v3.2.1 | [PCI.CW.1 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확합니다. | [CloudWatch.1] 루트 사용자 사용을 위한 로그 메트릭 필터 및 경보가 있는지 확인합니다. |
| PCI DSS v3.2.1 | PCI.DMS.1 Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다. | [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다. |
| PCI DSS v3.2.1 | PCI.EC2.1 EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다. | [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원 가능하도록 구성해서는 안 됩니다. |
| PCI DSS v3.2.1 | PCI.EC2.2 VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 금지해야 합니다. | [EC2.2] VPC 기본 보안 그룹은 인바운드 및 아웃바운드 트래픽을 허용해서는 안 됩니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| PCI DSS v3.2.1 | PCI.EC2.4 사용하지 않는 EC2 EIP를 제거해야 합니다. | [EC2.12] 사용하지 않는 Amazon EC2 EIP는 제거해야 합니다. |
| PCI DSS v3.2.1 | PCI.EC2.5 보안 그룹은 0.0.0.0/0에서 포트 22로의 수신을 허용해서는 안 됩니다. | [EC2.13] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 22로의 수신을 허용해서는 안 됩니다. |
| PCI DSS v3.2.1 | PCI.EC2.6 VPC 흐름 로깅은 모든 VPC에서 활성화되어야 합니다. | [EC2.6] VPC 플로 로깅은 모든 VPC에서 활성화되어야 합니다. |
| PCI DSS v3.2.1 | PCI.ELBv2.1 Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다. | [ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다. |
| PCI DSS v3.2.1 | PCI.ES.1 Elasticsearch 도메인은 VPC에 있어야 합니다. | [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다. |
| PCI DSS v3.2.1 | PCI.ES2 Elasticsearch 도메인에서 저장 시 암호화를 활성화해야 합니다. | [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다. |
| PCI DSS v3.2.1 | PCI.GuardDuty.1 GuardDuty가 활성화되어 있어야 합니다. | [GuardDuty.1] GuardDuty를 활성화해야 합니다. |
| PCI DSS v3.2.1 | PCI.IAM.1 IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다. | [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다. |
| PCI DSS v3.2.1 | PCI.IAM.2 IAM 사용자는 IAM 정책을 연결해서는 안 됩니다. | [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다. |
| PCI DSS v3.2.1 | PCI.IAM.3 IAM 정책은 전체 '*' 관리 권한을 허용해서는 안 됩니다. | [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다. |
| PCI DSS v3.2.1 | PCI.IAM.4 루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다. | [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| PCI DSS v3.2.1 | PCI.IAM.5 루트 사용자에 대해 가상 MFA를 활성화해야 합니다. | [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다. |
| PCI DSS v3.2.1 | PCI.IAM.6 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다. | [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다. |
| PCI DSS v3.2.1 | PCI.IAM.7 IAM 사용자 보안 인증은 미리 정의된 일수 내에 사용하지 않을 경우, 비활성화해야 합니다. | [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다. |
| PCI DSS v3.2.1 | PCI.IAM.8 IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다. | [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다. |
| PCI DSS v3.2.1 | PCI.KMS.1 고객 마스터 키(CMK) 교체가 활성화되어야 합니다. | [KMS.4]AWS KMS키 교체를 활성화해야 합니다. |
| PCI DSS v3.2.1 | PCI.Lambda.1 Lambda 함수는 퍼블릭 액세스를 금지해야 합니다. | [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다. |
| PCI DSS v3.2.1 | PCI.Lambda.2 Lambda 함수는 VPC에 있어야 합니다. | [Lambda.3] Lambda 함수는 VPC에 있어야 합니다. |
| PCI DSS v3.2.1 | PCI.OpenSearch.1 OpenSearch 도메인은 VPC에 있어야 합니다. | [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다. |
| PCI DSS v3.2.1 | PCI.Opensearch.2 EBS 스냅샷은 공개적으로 복원할 수 없어야 합니다. | [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다. |
| PCI DSS v3.2.1 | PCI.RDS.1 RDS 스냅샷은 비공개 상태여야 합니다. | [RDS.1] RDS 스냅샷은 비공개여야 합니다. |
| PCI DSS v3.2.1 | PCI.RDS.2 RDS DB 인스턴스는 퍼블릭 액세스를 금지해야 합니다. | [RDS.2] RDS DB 인스턴스는 PubliclyAccessible 구성으로 결정된 퍼블릭 액세스를 금지해야 합니다. |

| 표준 | 표준 제어 ID 및 제목 | 보안 제어 ID 및 제목 |
|---|---|---|
| PCI DSS v3.2.1 | PCI.Redshift.1 Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다. | [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다. |
| PCI DSS v3.2.1 | PCI.S3.1 S3 버킷은 퍼블릭 쓰기 액세스를 금지해야 합니다. | [S3.3] S3 범용 버킷은 공개 쓰기 액세스를 차단해야 합니다 |
| PCI DSS v3.2.1 | PCI.S3.2 S3 버킷은 퍼블릭 읽기 액세스를 금지해야 합니다. | [S3.2] S3 범용 버킷은 퍼블릭 읽기 액세스를 차단해야 합니다. |
| PCI DSS v3.2.1 | PCI.S3.3 S3 버킷에 교차 리전 복제가 활성화되어 있어야 합니다. | [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다 |
| PCI DSS v3.2.1 | PCI.S3.5 S3 버킷에는 SSL(Secure Socket Layer) 사용 요청이 필요합니다. | [S3.5] S3 범용 버킷에는 TLS 사용 요청이 필요합니다. |
| PCI DSS v3.2.1 | PCI.S3.6 S3 퍼블릭 액세스 차단 설정을 활성화해야 합니다. | [S3.1] S3 범용 버킷은 퍼블릭 액세스 차단 설정을 활성화해야 합니다 |
| PCI DSS v3.2.1 | PCI.SageMaker.1 Amazon SageMaker 노트북 인스턴스는 직접 인터넷에 액세스할 수 없어야 합니다. | [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다. |
| PCI DSS v3.2.1 | PCI.SSM.1 Systems Manager가 관리하는 EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다. | [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다. |
| PCI DSS v3.2.1 | PCI.SSM.2 Systems Manager에서 관리하는 EC2 인스턴스의 연결 규정 준수 상태는 COMPLIANT여야 합니다. | [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다. |
| PCI DSS v3.2.1 | PCI.SSM.3 EC2 인스턴스는에서 관리해야 합니다. AWS Systems Manager | [SSM.1] Amazon EC2 인스턴스는에서 관리해야 합니다.AWS Systems Manager |

통합을 위한 워크플로 업데이트

워크플로가 제어 조사 결과 중 어떤 필드의 특정 형식도 사용하지 않는 경우, 별도의 조치가 필요하지 않습니다.

이전 표에서 언급한 대로 워크플로가 제어 조사 결과 중 하나 이상의 필드의 특정 형식을 사용하는 경우, 워크플로를 업데이트해야 합니다. 예를 들어, 제어 ID가 CIS 2.7인 경우 AWS Lambda 함수 호출과 같은 특정 제어 ID에 대한 작업을 트리거한 Amazon EventBridge 규칙을 생성한 경우 해당 제어의 `Compliance.SecurityControlId` 필드 값CloudTrail.2,를 사용하도록 규칙을 업데이트합니다.

변경된 제어필드 또는 값을 사용하는 사용자 지정 인사이트를 생성한 경우, 새 필드 또는 값을 사용하도록 해당 인사이트를 업데이트해야 합니다.

## 필수 최상위 ASFF 속성

AWS Security Hub CSPM의 모든 결과에는 Security Finding 형식(ASFF)의 다음과 같은 최상위 속성이 필요합니다. 이러한 속성에 대한 자세한 내용은 AWS Security Hub API 참조의 AwsSecurityFinding 섹션을 참조하세요.

AwsAccountId

조사 결과가 적용되는 AWS 계정 ID입니다.

예제

```
"AwsAccountId": "111111111111"
```

CreatedAt

조사 결과로 캡처된 잠재적 보안 문제 또는 이벤트가 생성된 시점을 나타냅니다.

예제

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

설명

조사 결과에 대한 설명. 이 필드는 일반적인 표준 문안 텍스트 또는 조사 결과의 인스턴스에만 해당하는 세부 정보일 수 있습니다.

Security Hub CSPM이 생성하는 제어 조사 결과의 경우, 이 필드는 제어에 대한 설명을 제공합니다.

통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예제

```
"Description": "This AWS control checks whether AWS Config is enabled in the current
 account and Region."
```

GeneratorId

조사 결과를 생성했던 솔루션별 구성 요소(로직의 개별 단위)에 대한 식별자.

Security Hub CSPM이 생성하는 제어 조사 결과의 경우, 통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예제

```
"GeneratorId": "security-control/Config.1"
```

Id

조사 결과에 대한 제품별 식별자. Security Hub CSPM이 생성하는 제어 조사 결과에 대해 이 필드는 조사 결과 Amazon 리소스 이름(ARN)을 제공합니다.

통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예제

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/
ab6d6a26-a156-48f0-9403-115983e5a956"
```

ProductArn

제품이 Security Hub CSPM에 등록된 후 서드 파티 조사 결과 제품을 고유하게 식별하는 Security Hub CSPM에서 생성된 Amazon 리소스 이름(ARN)입니다.

이 필드의 형식은 `arn:`*`partition`*`:securityhub:`*`region`*`:`*`account-id`*`:product/`*`company-id`*`/`*`product-id`*입니다.

- Security Hub CSPM과 통합된 AWS 서비스 의 경우는 "aws"이어야 `company-id` 하고는 AWS 퍼블릭 서비스 이름이어야 `product-id` 합니다. 제품 및 서비스는 계정과 연결되지 않으므로 AWS ARN의 `account-id` 섹션이 비어 있습니다. Security Hub CSPM과 아직 통합되지 AWS 서비스 않은 섹션은 타사 제품으로 간주됩니다.
- 퍼블릭 제품의 경우, `company-id` 및 `product-id`은(는) 등록 시 지정된 ID 값이어야 합니다.

- 프라이빗 제품의 경우, `company-id`이(가) 계정 ID여야 합니다. `product-id`은(는) 예약어 '기본' 또는 등록 시 지정된 ID여야 합니다.

예제

```
// 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"
```

리소스

객체 `Resources` 배열은 조사 결과가 참조하는 리소스를 설명하는 AWS 리소스 데이터 유형 세트를 제공합니다. 필수 필드를 포함하여 `Resources` 객체에 포함될 수 있는 필드에 대한 자세한 내용은 AWS Security Hub API 참조의 Resource 섹션을 참조하세요. 특정의 `Resources` 객체 예제는 단원을 AWS 서비스참조하십시오Resources ASFF 객체.

예제

```
"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

조사 결과의 형식이 지정된 스키마 버전. 이 필드의 값은 AWS(으)로 식별되는 공식적으로 게시된 버전 중 하나여야 합니다. 현재 릴리스에서 AWS Security Finding 형식 스키마 버전은 입니다`2018-10-08`.

예제

```
"SchemaVersion": "2018-10-08"
```

### 심각도

조사 결과의 중요성을 정의합니다. 이 객체에 대한 자세한 내용은 AWS Security Hub API 참조의 `Severity` 섹션을 참조하세요.

Severity은(는) 조사 결과의 최상위 객체이자 FindingProviderFields 객체 아래에 중첩되어 있습니다.

조사 결과의 최상위 Severity 객체 값은 BatchUpdateFindings API를 사용해서만 업데이트해야 합니다.

심각도 정보를 제공하려면 조사 결과 공급자가 BatchImportFindings API 요청 시 FindingProviderFields 아래의 Severity 객체를 업데이트해야 합니다.
새로운 조사 결과에 대한 BatchImportFindings 요청이 Label만 제공하거나 Normalized만 제공하는 경우, Security Hub CSPM은 다른 필드의 값을 자동으로 채웁니다. Product 및 Original 필드도 채워질 수 있습니다.

최상위 Finding.Severity 객체가 존재하지만 Finding.FindingProviderFields가 존재하지 않는 경우, Security Hub CSPM은 FindingProviderFields.Severity 객체를 생성하고 Finding.Severity object 전체를 여기에 복사합니다. 이렇게 하면 최상위 Severity 객체를 덮어쓰더라도 공급자가 제공하는 원본 세부 정보가 FindingProviderFields.Severity 구조 내에 유지됩니다.

조사 결과의 심각도는 관련 자산 또는 기본 리소스의 중요성을 고려하지 않습니다. 중요성은 조사 결과와 관련된 리소스의 중요도 수준으로 정의됩니다. 예를 들어, 미션 크리티컬 애플리케이션과 관련된 리소스는 비프로덕션 테스트와 관련된 리소스보다 중요도가 더 높습니다. 리소스 중요성에 대한 정보를 캡처하려면 Criticality 필드를 사용합니다.

조사 결과의 기본 심각도 점수를 ASFF의 Severity.Label 값으로 변환할 때는 다음 지침을 사용하는 것이 좋습니다.

- INFORMATIONAL – 이 범주에는 PASSED, WARNING, 또는 NOT AVAILABLE 조사 결과 또는 민감한 데이터 식별에 대한 결과가 포함될 수 있습니다.
- LOW – 향후 손상으로 이어질 수 있는 조사 결과. 예를 들어, 이 범주에는 취약성, 구성 약점, 노출된 비밀번호가 포함될 수 있습니다.
- MEDIUM – 활성 상태의 손상과 관련이 있지만 공격자가 목적을 달성했다는 증거는 없는 조사 결과. 예를 들어, 이 범주에는 맬웨어 활동, 해킹 활동 및 비정상적인 동작 감지가 포함될 수 있습니다.
- HIGH 또는 CRITICAL – 데이터 손실, 위반 행위 또는 서비스 거부 등 공격자의 목적 달성을 나타내는 조사 결과.

예제

```
"Severity": {
```

```
    "Label": "CRITICAL",
    "Normalized": 90,
    "Original": "CRITICAL"
}
```

제목

조사 결과의 제목. 이 필드는 일반적인 표준 문안 텍스트 또는 조사 결과의 이 인스턴스에만 해당하는 세부 정보를 포함할 수 있습니다.

제어 조사 결과의 경우, 이 필드는 제어의 제목을 제공합니다. 통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

예제

```
"Title": "AWS Config should be enabled"
```

유형

조사 결과를 분류하는 *namespace*/*category*/*classifier* 형식으로 구성된 하나 이상의 조사 결과 유형. 통합 제어 조사 결과를 켜면 이 필드는 표준을 참조하지 않습니다.

Types는 BatchUpdateFindings API를 사용해서만 업데이트해야 합니다.

Types에 대한 값을 입력하고자 하는 조사 결과 공급자는 FindingProviderFields 아래의 Types 속성을 사용해야 합니다.

다음 목록에서 1단계 글머리 기호는 네임스페이스이고 2단계 글머리 기호는 범주이며 3단계 글머리 기호는 분류자입니다. 조사 결과 공급자는 정의된 네임스페이스를 사용하여 조사 결과를 정렬하고 그룹화하는 것이 좋습니다. 정의된 범주와 분류자를 사용할 수도 있지만 필수는 아닙니다. 소프트웨어 및 구성 점검 네임스페이스에만 분류자가 정의되어 있습니다.

네임스페이스/범주/분류자에 대한 부분 경로를 정의할 수 있습니다. 예를 들어, 다음의 조사 결과 유형은 모두 유효합니다.

- TTP
- TTPs/Defense Evasion
- TTPs/Defense Evasion/CloudTrailStopped

다음 목록의 전술, 기술 및 절차(TTP) 범주는 MITER ATT & CK MatrixTM에 맞춰 정렬됩니다. Unusual Behaviors 네임스페이스는 일반적인 통계 이상과 같은 일반적인 비정상적인 동작을 반영하며 특정

TTP에 맞게 정렬되지 않습니다. 그러나 비정상 동작과 TTP 조사 결과 유형을 모두 사용하여 조사 결과를 분류할 수 있습니다.

네임스페이스, 범주, 분류자 목록:

- 소프트웨어 및 구성 점검
  - 취약성
    - CVE
  - AWS 보안 모범 사례
    - 네트워크 연결성
    - 실행 시간 행동 분석
  - 산업 및 규제 표준
    - AWS 기본 보안 모범 사례
    - CIS 호스트 강화 Benchmark
    - CIS AWS 파운데이션 벤치마크
    - PCI-DSS
    - Cloud Security Alliance(CSA) 규제
    - ISO 90001 규제
    - ISO 27001 규제
    - ISO 27017 규제
    - ISO 27018 규제
    - SOC 1
    - SOC 2
    - HIPAA 규제(미국)
    - NIST 800-53 규제(미국)
    - NIST CSF 규제(미국)
    - IRAP 규제(호주)
    - K-ISMS 규제(한국)
    - MTCS 규제(싱가포르)
    - FISC 규제(일본)
    - My Number Act 규제(일본)
    - ENS 규제(스페인)

    - Cyber Essentials Plus 규제(영국)
    - G-Cloud 규제(영국)
    - C5 규제(독일)
    - IT-Grundschutz 규제(독일)
    - GDPR 규제(유럽)
    - TISAX 규제(유럽)
  - 패치 관리
- TTP
  - 초기 액세스
  - Execution
  - Persistence
  - 권한 에스컬레이션
  - 방어 회피
  - 자격 증명 액세스
  - Discovery
  - 수평 이동
  - 수집
  - 명령 및 제어
- 효과
  - 데이터 노출
  - 데이터 유출
  - 데이터 폐기
  - 서비스 거부 공격
  - 리소스 소비
- 비정상 동작
  - 애플리케이션
  - 네트워크 흐름
  - IP 주소
  - User



  - VM

  - 컨테이너
  - 서버리스
  - 프로세스
  - Database
  - 데이터
- 민감한 데이터 식별
  - PII
  - 암호
  - 법적 고지
  - 금융
  - 보안
  - 업무

예제

```
"Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
]
```

UpdatedAt

조사 결과 공급자가 조사 결과 기록을 마지막으로 업데이트한 시기를 나타냅니다.

이 타임스탬프는 조사 결과 기록이 마지막으로 업데이트되었거나 가장 최근에 업데이트된 시간을 반영합니다. 따라서 이벤트 또는 취약성이 마지막으로 관찰된 시점 또는 가장 최근에 관찰된 시점을 반영하는 `LastObservedAt` 타임스탬프와 다를 수 있습니다.

조사 결과 기록을 업데이트할 때 이 타임스탬프를 현재 타임스탬프로 업데이트해야 합니다. 조사 결과 기록을 생성하면 `CreatedAt` 및 `UpdatedAt` 타임스탬프는 같아야 합니다. 조사 결과 기록을 업데이트한 후 이 필드의 값은 이전에 포함했던 모든 값보다 최근이어야 합니다.

단, `BatchUpdateFindings` 작업을 사용하여 `UpdatedAt`를 업데이트할 수는 없습니다. `BatchImportFindings` 작업을 사용해야만 업데이트할 수 있습니다.

예제

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

## 선택적 최상위 ASFF 속성

AWS Security Hub CSPM의 조사 결과에 대해 Security Finding Format(ASFF)의 다음 최상위 속성은 선택 사항입니다. 이러한 속성에 대한 자세한 내용은 AWS Security Hub API 참조의 AwsSecurityFinding 섹션을 참조하세요.

### 작업

`Action` 객체는 리소스에 영향을 주거나 리소스에 대해 취해진 작업에 대한 세부 정보를 제공합니다.

예제

```
"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

조사 결과가 적용되는 AWS 계정 이름입니다.

예제

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

조사 결과를 생성했던 제품의 회사 이름. 제어 기반 조사 결과의 경우 회사는 입니다 AWS.

Security Hub CSPM은 각 조사 결과에 대해 이 속성을 자동으로 채웁니다. `BatchImportFindings` 또는 `BatchUpdateFindings`을(를) 사용하여 업데이트할 수 없습니다. 사용자 지정 통합을 사용하는 경우는 예외입니다. the section called “사용자 지정 제품 통합”을(를) 참조하세요.

Security Hub CSPM 콘솔을 사용하여 회사 이름을 기준으로 조사 결과를 필터링할 때는 이 속성을 사용합니다. Security Hub CSPM API를 사용하여 조사 결과를 제품 이름별로 필터링할 때는 `ProductFields` 아래의 `aws/securityhub/CompanyName` 속성을 사용합니다. Security Hub CSPM은 이러한 두 속성을 동기화하지 않습니다.

예제

```
"CompanyName": "AWS"
```

규정 준수

`Compliance` 객체는 일반적으로 적용 가능한 표준 및 제어 검사 상태와 같은 제어 조사 결과에 대한 세부 정보를 제공합니다.

예제

```
"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."
        }
    ]
}
```

신뢰도

조사 결과가 식별하고자 하는 동작이나 문제를 정확하게 식별할 가능성.

`Confidence`은(는) `BatchUpdateFindings`을(를) 사용해서만 업데이트해야 합니다.

Confidence에 대한 값을 입력하고자 하는 조사 결과 공급자는 FindingProviderFields 아래의 Confidence 속성을 사용해야 합니다. the section called “FindingProviderFields(으)로 조사 결과 업데이트” 섹션을 참조하세요.

Confidence은(는) 비율 척도를 사용하여 0~100점으로 채점됩니다. 0은 0% 신뢰도를 의미하고, 100은 100% 신뢰도를 의미합니다. 예를 들어, 실제 유출이 확인되지 않았기 때문에 네트워크 트래픽의 통계적 편차를 기반으로 한 데이터 유출 감지는 신뢰도가 낮습니다.

예제

```
"Confidence": 42
```

중요도

조사 결과와 관련된 리소스에 할당된 중요도 수준.

Criticality은(는) BatchUpdateFindings API 작업을 직접 호출해서만 업데이트해야 합니다. BatchImportFindings(으)로 이 객체를 업데이트하지 마세요.

Criticality에 대한 값을 입력하고자 하는 조사 결과 공급자는 FindingProviderFields 아래의 Criticality 속성을 사용해야 합니다. the section called “FindingProviderFields(으)로 조사 결과 업데이트” 섹션을 참조하세요.

Criticality은(는) 정수만 지원하는 비율 척도를 사용하여 0~100점을 기준으로 점수가 부여됩니다. 0점은 기본 리소스에 중요성이 없음을 의미하며 100점은 가장 중요한 리소스에 예약됩니다.

각 리소스에 Criticality을(를) 할당할 때는 다음 사항을 고려하세요.

- 영향을 받는 리소스에 민감한 데이터(예제: PII가 있는 S3 버킷)가 포함되어 있습니까?
- 영향을 받는 리소스에서 악의적 공격자가 더 깊이 액세스하거나 또 다른 악의적 활동(예제: 시스템 관리자 계정 공격)을 수행할 가능성이 확대될 수 있습니까?
- 리소스가 비즈니스에 중요한 자산(예제: 손상될 경우, 수익에 상당한 영향을 미칠 수 있는 핵심 비즈니스 시스템)입니까?

다음 지침을 적용할 수 있습니다.

- 미션 크리티컬 시스템을 지원하거나 매우 민감한 데이터를 포함하는 리소스는 75~100점 범위에서 점수를 매길 수 있습니다.
- 중요한(핵심적이지는 않은) 데이터를 지원하거나 다소 중요한 데이터를 포함하는 리소스는 25~74점 범위에서 점수를 매길 수 있습니다.

- 중요하지 않은 시스템을 지원하거나 중요하지 않은 데이터를 포함하는 리소스는 반드시 0~24점 범위로 점수를 매겨야 합니다.

예제

```
"Criticality": 99
```

탐지

`Detection` 객체는 Amazon GuardDuty Extended Threat Detection의 공격 시퀀스 조사 결과에 대한 세부 정보를 제공합니다. GuardDuty는 여러 이벤트가 잠재적으로 의심스러운 활동과 일치할 때 공격 시퀀스 조사 결과를 생성합니다. AWS Security Hub CSPM에서 GuardDuty 공격 시퀀스 결과를 수신하려면 계정에서 GuardDuty가 활성화되어 있어야 합니다. 자세한 내용은 Amazon GuardDuty 사용 설명서의 Amazon GuardDuty Extended Threat Detection을 참조하세요.

예제

```
"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`에는 다음 속성이 포함될 수 있습니다.

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

앞의 필드는 FindingProviderFields 객체 아래에 중첩되지만 최상위 ASFF 필드와 동일한 이름의 아날로그가 있습니다. 조사 결과 공급자가 새로운 조사 결과를 Security Hub CSPM으로 전송하면 Security Hub CSPM은 해당 최상위 필드를 기반으로 FindingProviderFields 객체가 비어 있는 경우, 객체를 자동으로 채웁니다.

조사 결과 공급자는 Security Hub CSPM API의 BatchImportFindings 작업을 사용하여 FindingProviderFields를 업데이트할 수 있습니다. 조사 결과 공급자가 BatchUpdateFindings(으)로 이 객체를 업데이트할 수 없습니다.

Security Hub CSPM이 BatchImportFindings에서 FindingProviderFields로의 업데이트와 해당 최상위 속성을 처리하는 방법에 대한 자세한 내용은 the section called “FindingProviderFields(으)로 조사 결과 업데이트” 섹션을 참조하세요.

고객은 BatchUpdateFindings 작업을 사용하여 최상위 필드를 업데이트할 수 있습니다. 고객은 FindingProviderFields을(를) 업데이트할 수 없습니다.

예제

```
"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

조사 결과로 캡처된 잠재적 보안 문제 또는 이벤트가 처음 발견된 시점을 나타냅니다.

이 타임스탬프는 이벤트 또는 취약성이 처음 관찰된 시간을 표시합니다. 따라서, 이 조사 결과 기록이 생성된 시점을 반영하는 `CreatedAt` 타임스탬프와 다를 수 있습니다.

Security Hub CSPM이 생성하고 업데이트하는 제어 조사 결과의 경우, 이 타임스탬프는 리소스의 규정 준수 상태가 가장 최근에 변경된 시점을 나타낼 수도 있습니다. 다른 조사 결과 유형의 경우, 이 타임스탬프는 조사 결과 레코드의 업데이트 간에는 변하지 않아야 하지만, 보다 정확한 타임스탬프가 결정되면 업데이트할 수 있습니다.

예제

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

조사 결과로 캡처된 잠재적 보안 문제 또는 이벤트가 보안 조사 결과 제품에 의해 가장 최근에 발견된 시점을 나타냅니다.

이 타임스탬프는 이벤트 또는 취약성이 마지막으로 또는 가장 최근에 관찰된 시간을 표시합니다. 따라서, 이 조사 결과 기록이 마지막으로 업데이트된 시점 또는 가장 최근에 업데이트된 시점을 반영하는 `UpdatedAt` 타임스탬프와 다를 수 있습니다.

이 타임스탬프를 입력할 수는 있지만 최초 관찰 시 필수적이지는 않습니다. 최초 관찰 시 이 필드를 입력하는 경우, 이 타임스탬프는 `FirstObservedAt` 타임스탬프와 동일해야 합니다. 조사 결과가 관찰될 때마다 마지막으로 또는 가장 최근에 관찰된 타임스탬프를 반영하여 이 필드를 업데이트해야 합니다.

예제

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

`Malware` 객체는 조사 결과와 관련된 악성코드 목록을 제공합니다.

예제

```
"Malware": [
    {
        "Name": "Stringler",
        "Type": "COIN_MINER",
        "Path": "/usr/sbin/stringler",
        "State": "OBSERVED"
    }
]
```

### Network(사용 중지)

Network 객체는 조사 결과에 대한 네트워크 관련 정보를 제공합니다.

이 객체는 사용 중지되었습니다. 이 데이터를 입력하려면 데이터를 Resources의 리소스에 매핑하거나 Action 객체를 사용할 수 있습니다.

예제

```
"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

NetworkPath 객체는 조사 결과와 관련된 네트워크 경로에 대한 정보를 제공합니다.
NetworkPath의 각 항목은 경로의 구성 요소를 나타냅니다.

예제

```
"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" ]
            }
        }
     }
]
```

참고

Note 객체는 조사 결과에 추가할 수 있는 사용자 정의 메모를 지정합니다.

조사 결과 공급자는 조사 결과에 대한 초기 메모를 입력할 수 있지만 그 후에 메모를 추가할 수는 없습니다. 메모는 BatchUpdateFindings을(를) 사용해서만 업데이트할 수 있습니다.

예제

```
"Note": {
    "Text": "Don't forget to check under the mat.",
    "UpdatedBy": "jsmith",
    "UpdatedAt": "2018-08-31T00:15:09Z"
}
```

PatchSummary

이 PatchSummary 객체는 선택한 규정 준수 표준을 기준으로 인스턴스의 패치 규정 준수 상태를 요약하여 제공합니다.

예제

```
"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"
}
```

프로세스

Process 객체는 조사 결과에 대한 프로세스 관련 세부 정보를 제공합니다.

예제:

```
"Process": {
    "LaunchedAt": "2018-09-27T22:37:31Z",
    "Name": "syslogd",
    "ParentPid": 56789,
    "Path": "/usr/sbin/syslogd",
    "Pid": 12345,
    "TerminatedAt": "2018-09-27T23:37:31Z"
```

```
}
```

ProcessedAt

Security Hub CSPM이 조사 결과를 수신하고 처리를 시작한 시점을 나타냅니다.

이는 조사 결과 공급자와 보안 문제 및 조사 결과의 상호 작용과 관련된 필수 타임스탬프인 `CreatedAt` 및 `UpdatedAt`와(과) 다릅니다. `ProcessedAt` 타임스탬프는 Security Hub CSPM이 조사 결과를 처리하기 시작하는 시점을 나타냅니다. 처리가 완료된 후 사용자 계정에 조사 결과가 나타납니다.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

보안 조사 결과 제품에 정의된 AWS 보안 조사 결과 형식의 일부가 아닌 추가 솔루션별 세부 정보가 포함될 수 있는 데이터 유형입니다.

Security Hub CSPM 제어에서 생성된 조사 결과의 경우, 제어에 대한 정보가 `ProductFields`에 포함됩니다. the section called “제어 조사 결과 생성 및 업데이트”을(를) 참조하세요.

이 필드에는 중복 데이터가 포함되어서는 안 되며 AWS Security Finding 형식 필드와 충돌하는 데이터가 포함되어서는 안 됩니다.

"`aws/`" 접두사는 AWS 제품 및 서비스에 대해서만 예약된 네임스페이스를 나타내며 타사 통합의 결과와 함께 제출해서는 안 됩니다.

필수는 아니지만 제품은 필드 이름의 형식을 `company-id/product-id/field-name`(으)로 지정해야 합니다. 여기서 `company-id`와(과) `product-id`은(는) 조사 결과의 `ProductArn`에 입력된 것과 일치합니다.

`Archival`을 참조하는 필드는 Security Hub CSPM이 기존 조사 결과를 보관할 때 사용됩니다. 예를 들어, Security Hub CSPM은 제어 또는 표준을 비활성화할 때와 통합 제어 조사 결과를 켜거나 끌 때 기존 조사 결과를 보관합니다.

이 필드에는 조사 결과를 생성했던 제어를 포함하는 표준에 대한 정보도 포함될 수 있습니다.

예제

```
"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

조사 결과를 생성했던 제품의 이름을 입력합니다. 제어 기반 조사 결과의 경우, 제품 이름은 Security Hub CSPM입니다.

Security Hub CSPM은 각 조사 결과에 대해 이 속성을 자동으로 채웁니다. `BatchImportFindings` 또는 `BatchUpdateFindings`을(를) 사용하여 업데이트할 수 없습니다. 사용자 지정 통합을 사용하는 경우는 예외입니다. the section called “사용자 지정 제품 통합”을(를) 참조하세요.

Security Hub CSPM 콘솔을 사용하여 제품 이름을 기준으로 조사 결과를 필터링할 때는 이 속성을 사용합니다.

Security Hub CSPM API를 사용하여 조사 결과를 제품 이름별로 필터링할 때는 `ProductFields` 아래의 `aws/securityhub/ProductName` 속성을 사용합니다.

Security Hub CSPM은 이러한 두 속성을 동기화하지 않습니다.

RecordState

조사 결과의 기록 상태를 입력합니다.

기본적으로 서비스에서 처음 생성된 조사 결과는 `ACTIVE`(으)로 간주됩니다.

`ARCHIVED` 상태는 조사 결과를 보기에서 숨겨야 함을 나타냅니다. 보관된 조사 결과는 즉시 삭제되지 않습니다. 이를 검색, 검토 및 보고할 수 있습니다. Security Hub CSPM은 연결된 리소스가 삭제되거나, 리소스가 존재하지 않거나, 제어가 비활성화된 경우, 제어 기반 조사 결과를 자동으로 보관합니다.

`RecordState`는 조사 결과 공급자를 위한 것으로, `BatchImportFindings` 작업을 사용해야만 업데이트할 수 있습니다. `BatchUpdateFindings` 작업을 사용하면 업데이트할 수 없습니다.

조사 결과에 대한 조사 상태를 추적하려면 RecordState 대신 Workflow을(를) 사용하세요.

레코드 상태가 ARCHIVED에서 ACTIVE로 변경되고 조사 결과의 워크플로 상태가 NOTIFIED 또는 RESOLVED인 경우, Security Hub CSPM은 자동으로 워크플로 상태를 NEW로 변경합니다.

예제

```
"RecordState": "ACTIVE"
```

리전

결과가 생성된 AWS 리전 를 지정합니다.

Security Hub CSPM은 각 조사 결과에 대해 이 속성을 자동으로 채웁니다. BatchImportFindings 또는 BatchUpdateFindings을(를) 사용하여 업데이트할 수 없습니다.

예제

```
"Region": "us-west-2"
```

RelatedFindings

현재 조사 결과와 관련된 조사 결과 목록을 입력합니다.

RelatedFindings는 BatchUpdateFindings API 작업으로만 업데이트해야 합니다. BatchImportFindings로 이 객체를 업데이트하면 안 됩니다.

BatchImportFindings 요청의 경우, 조사 결과 공급자는 FindingProviderFields 아래의 RelatedFindings 객체를 사용해야 합니다.

RelatedFindings 속성 설명을 보려면 AWS Security Hub API 참조의 RelatedFinding를 참조하세요.

예제

```
"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

### 예제

```
"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"
                    }
```

```
                ]
            }
        ]
    }
}
```

### 문제 해결

Remediation 객체는 조사 결과를 처리하기 위해 권장되는 문제 해결 단계에 대한 정보를 제공합니다.

#### 예제

```
"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"
    }
}
```

### Sample

조사 결과가 샘플 조사 결과인지 여부를 지정합니다.

```
"Sample": true
```

### SourceUrl

SourceUrl 객체는 조사 결과 제품의 현재 조사 결과에 대한 페이지로 연결되는 URL을 제공합니다.

```
"SourceUrl": "http://sourceurl.com"
```

### ThreatIntelIndicators

ThreatIntelIndicator 객체는 조사 결과와 관련된 위협 인텔리전스 세부 정보를 제공합니다.

#### 예제

```
"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",
  }
]
```

### Threats

Threats 객체는 조사 결과로 탐지된 위협에 대한 세부 정보를 제공합니다.

예제

```
"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

조사 결과와 연관된 이름/값 문자열 페어의 목록을 입력합니다. 이는 조사 결과에 추가되는 사용자 정의 필드입니다. 이러한 필드는 특정 구성을 통해 자동으로 생성될 수 있습니다.

조사 결과 공급자는 제품이 생성하는 데이터에 이 필드를 사용해서는 안 됩니다. 대신 결과 공급자는 표준 AWS 보안 결과 형식 `ProductFields` 필드에 매핑되지 않는 데이터에 필드를 사용할 수 있습니다.

이 필드는 BatchUpdateFindings을(를) 사용해서만 업데이트할 수 있습니다.

예제

```
"UserDefinedFields": {
    "reviewedByCio": "true",
    "comeBackToLater": "Check this again on Monday"
```

```
}
```

VerificationState

조사 결과의 진실성을 입력합니다. 조사 결과 제품은 이 필드에 UNKNOWN 값을 입력할 수 있습니다. 조사 결과 제품의 시스템에 의미 있는 유사점이 있는 경우, 조사 결과 제품은 이 필드의 값을 입력해야 합니다. 이 필드는 일반적으로 사용자가 결과를 조사한 이후의 사용자 결정 또는 작업으로 채워집니다.

조사 결과 공급자는 이 속성의 초기 값을 입력할 수 있지만 그 이후에는 업데이트할 수 없습니다. 이 속성은 BatchUpdateFindings을(를) 사용해서만 업데이트할 수 있습니다.

```
"VerificationState": "Confirmed"
```

취약성

Vulnerabilities 객체는 조사 결과와 관련된 취약성 목록을 제공합니다.

예제

```
"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"
            }
        ]
    }
]
```

### 워크플로

Workflow 객체는 결과의 조사 상태에 대한 정보를 제공합니다.

이 필드는 고객이 수정, 오케스트레이션 및 티켓 작성 도구와 함께 사용하기 위한 것입니다. 조사 결과 공급자를 위한 용도는 아닙니다.

`BatchUpdateFindings`을(를) 사용하여 `Workflow` 필드를 업데이트할 수만 있습니다. 고객은 콘솔에서 업데이트할 수도 있습니다. the section called "조사 결과에 대한 워크플로 상태 설정" 섹션을 참조하세요.

예제

```
"Workflow": {
    "Status": "NEW"
}
```

WorkflowState(사용 중지됨)

이 객체는 사용 중지되었으며 `Workflow` 객체의 `Status` 필드로 대체되었습니다.

이 필드는 조사 결과의 워크플로 상태를 제공합니다. 조사 결과 제품은 이 필드에 `NEW` 값을 입력할 수 있습니다. 조사 결과 제품의 시스템에 의미 있는 유사점이 있는 경우, 조사 결과 제품은 이 필드의 값을 입력할 수 있습니다.

예제

```
"WorkflowState": "NEW"
```

## Resources ASFF 객체

AWS 보안 조사 결과 형식(ASFF)에서 `Resources` 객체는 조사 결과와 관련된 리소스에 대한 정보를 제공합니다. 여기에는 최대 32개의 리소스 객체로 구성된 배열이 포함됩니다. 리소스 이름의 형식을 결정하려면 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요. 각 리소스 객체의 예제를 보려면 다음 목록에서 리소스를 선택하세요.

주제

- ASFF의 리소스 속성
- AwsAmazonMQ ASFF의 리소스
- AwsApiGateway ASFF의 리소스
- AwsAppSync ASFF의 리소스
- AwsAthena ASFF의 리소스
- AwsAutoScaling ASFF의 리소스

- AwsBackup ASFF의 리소스
- AwsCertificateManager ASFF의 리소스
- AwsCloudFormation ASFF의 리소스
- AwsCloudFront ASFF의 리소스
- AwsCloudTrail ASFF의 리소스
- AwsCloudWatch ASFF의 리소스
- AwsCodeBuild ASFF의 리소스
- AwsDms ASFF의 리소스
- AwsDynamoDB ASFF의 리소스
- AwsEc2 ASFF의 리소스
- AwsEcr ASFF의 리소스
- AwsEcs ASFF의 리소스
- AwsEfs ASFF의 리소스
- AwsEks ASFF의 리소스
- AwsElasticBeanstalk ASFF의 리소스
- AwsElasticSearch ASFF의 리소스
- AwsElb ASFF의 리소스
- AwsEventBridge ASFF의 리소스
- AwsGuardDuty ASFF의 리소스
- AwsIam ASFF의 리소스
- AwsKinesis ASFF의 리소스
- AwsKms ASFF의 리소스
- AwsLambda
- AwsMsk ASFF의 리소스
- AwsNetworkFirewall ASFF의 리소스
- AwsOpenSearchService ASFF의 리소스
- AwsRds ASFF의 리소스
- AwsRedshift ASFF의 리소스
- AwsRoute53 ASFF의 리소스
- AwsS3 ASFF의 리소스

- AwsSageMaker ASFF의 리소스
- AwsSecretsManager ASFF의 리소스
- AwsSns ASFF의 리소스
- AwsSqs ASFF의 리소스
- AwsSsm ASFF의 리소스
- AwsStepFunctions ASFF의 리소스
- AwsWaf ASFF의 리소스
- AwsXray ASFF의 리소스
- ASFF의 CodeRepository 객체
- ASFF의 Container 객체
- ASFF의 Other 객체

### ASFF의 리소스 속성

다음은 AWS Security Finding 형식(ASFF)의 `Resources` 객체에 대한 설명과 예제입니다. 필드에 대한 자세한 내용은 리소스 섹션을 참조하세요.

#### ApplicationArn

조사 결과와 관련된 애플리케이션의 Amazon 리소스 이름(ARN)을 식별합니다.

예제

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/
SampleApp/1234567890abcdef0"
```

#### ApplicationName

조사 결과와 관련된 애플리케이션의 이름을 식별합니다.

예제

```
"ApplicationName": "SampleApp"
```

#### DataClassification

이 DataClassification 필드는 리소스에서 감지된 민감한 데이터에 대한 정보를 제공합니다.

## 예제

```
"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
        }
    }
}
```

### Details

이 Details 필드는 적절한 객체를 사용하는 단일 리소스에 대한 추가 정보를 제공합니다. `Resources` 객체의 개별 리소스 객체에 각 리소스를 입력해야 합니다.

단, 조사 결과 크기가 최대 240KB를 초과하는 경우, 해당 `Details` 객체는 조사 결과에서 제거됩니다. AWS Config 규칙을 사용하는 제어 조사 결과의 경우 AWS Config 콘솔에서 리소스 세부 정보를 볼 수 있습니다.

Security Hub CSPM은 지원되는 리소스 유형에 사용할 수 있는 리소스 세부 정보 세트를 제공합니다. 이러한 세부 정보는 `Type` 객체 값에 해당합니다. 가능한 경우, 항상 제공된 유형을 사용하세요.

예를 들어, 리소스가 S3 버킷인 경우, 리소스 `Type`을(를) `AwsS3Bucket`(으)로 설정하고 `AwsS3Bucket` 객체에 리소스 세부 정보를 제공합니다.

`Other` 객체를 사용하여 사용자 지정 필드 및 값을 입력할 수 있습니다. 다음과 같은 경우, `Other` 객체를 사용합니다.

- 리소스 유형(리소스 값 `Type`)에는 해당하는 세부 정보 객체가 없습니다. 리소스에 대한 세부 정보를 입력하려면 `Other` 객체를 사용합니다.
- 리소스 유형의 객체에 채우려는 모든 필드가 포함되어 있지 않습니다. 이 경우, 리소스 유형의 세부 정보 객체를 사용하여 사용 가능한 필드를 채웁니다. `Other` 객체를 사용하여 유형별 하위 필드에 없는 필드를 채웁니다.
- 리소스 유형이 제공된 유형 중 하나가 아닙니다. 이 경우, `Resource.Type`을(를) `Other`(으)로 설정하고 `Other` 객체를 사용하여 세부 정보를 채웁니다.

#### 예제

```
"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

주어진 리소스 유형에 대한 식별자입니다.

Amazon AWS 리소스 이름(ARNs)으로 식별되는 리소스의 경우 ARN입니다.

ARNs이 없는 AWS 리소스의 경우 리소스를 생성한 서비스에서 AWS 정의한 식별자입니다.

리소스AWS 가 아닌 경우 리소스와 연결된 고유 식별자입니다.

예제

```
"Id": "arn:aws:s3:::amzn-s3-demo-bucket"
```

Partition

리소스가 있는 파티션입니다. 파티션은의 그룹입니다 AWS 리전. 각 AWS 계정 는 하나의 파티션으로 범위가 지정됩니다.

지원되는 파티션은 다음과 같습니다.

- `aws` – AWS 리전
- `aws-cn` - 중국 리전
- `aws-us-gov` – AWS GovCloud (US) Region

예제

```
"Partition": "aws"
```

리전

이 리소스 AWS 리전 가 있는의 코드입니다. 리전 코드 목록은 리전 엔드포인트를 참조하세요.

예제

```
"Region": "us-west-2"
```

ResourceRole

조사 결과에서 리소스의 역할을 식별합니다. 리소스는 조사 결과 활동의 대상이거나 활동을 수행한 행위자입니다.

예제

```
"ResourceRole": "target"
```

Tags

이 필드는 조사 결과에 관련된 리소스에 대한 태그 키 및 값 정보를 제공합니다. 태깅 API의 `GetResources` 작업에서 지원하는 리소스에 AWS Resource Groups 태깅할 수 있습니다. Security Hub CSPM은 서비스 연결 역할을 통해이 작업을 호출하고 AWS Security Finding Format(ASFF) `Resource.Id` 필드가 리소스 ARN으로 채워진 경우 AWS 리소스 태그를 검색합니다. 유효하지 않은 리소스 ID는 무시됩니다.

통합 AWS 서비스 및 타사 제품의 결과를 포함하여 Security Hub CSPM이 수집하는 결과에 리소스 태그를 추가할 수 있습니다.

태그를 추가하면 조사 결과가 처리된 시점에 리소스와 연결된 태그가 처리되었다는 것을 알려줍니다. 연결된 태그가 있는 리소스에 대해서만 Tags 속성을 포함합니다. 리소스에 연결된 태그가 없는 경우, 조사 결과에 Tags 속성을 포함하지 마세요.

조사 결과에 리소스 태그를 포함하면 데이터 보강 파이프라인을 구축하거나 보안 조사 결과의 메타데이터를 수동으로 보강할 필요가 없습니다. 태그를 사용하여 조사 결과 및 인사이트를 검색 또는 필터링하고 자동화 규칙을 생성할 수도 있습니다.

태그에 적용되는 제한에 대한 자세한 내용은 태그 이름 지정 제한 및 요구 사항 섹션을 참조하세요.

이 필드의 AWS 리소스에 있는 태그만 제공할 수 있습니다. AWS Security Finding 형식에 정의되지 않은 데이터를 제공하려면 Other 세부 정보 하위 필드를 사용합니다.

예제

```
"Tags": {
    "billingCode": "Lotus-1-2-3",
    "needsPatching": "true"
}
```

Type

세부 정보가 입력되는 리소스 유형입니다.

가능한 경우, 항상 AwsEc2Instance 또는 AwsS3Bucket과 같은 제공된 리소스 유형 중 하나를 사용하세요.

리소스 유형이 제공된 리소스 유형과 일치하지 않는 경우, 리소스 Type을 Other로 설정하고 Other 세부 정보 하위 필드를 사용하여 세부 정보를 채웁니다.

지원되는 값은 리소스에 나열되어 있습니다.

예제

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ ASFF의 리소스

다음은 AwsAmazonMQ 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsAmazonMQBroker

AwsAmazonMQBroker은(는) Amazon MQ에서 실행하는 메시지 브로커 환경인 Amazon MQ 브로커에 대한 정보를 제공합니다.

다음 예제는 AwsAmazonMQBroker 객체에 대한 ASFF를 보여 줍니다. AwsAmazonMQBroker 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AWSAmazonMQBroker를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsApiGateway 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsApiGatewayRestApi

이 AwsApiGatewayRestApi 객체에는 Amazon API Gateway 버전 1에 있는 REST API에 대한 정보가 들어 있습니다.

다음은 AWS Security Finding Format(ASFF)에서 AwsApiGatewayRestApi 조사 결과의 예제입니다. AwsApiGatewayRestApi 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsApiGatewayRestApiDetails 세부 정보를 참조하세요.

예제

```
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

`AwsApiGatewayStage` 객체는 버전 1 Amazon API Gateway 단계에 대한 정보를 제공합니다.

다음은 AWS Security Finding Format(ASFF)에서 `AwsApiGatewayStage` 조사 결과의 예제입니다. `AwsApiGatewayStage` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsApiGatewayStageDetails 세부 정보를 참조하세요.

예제

```
"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

`AwsApiGatewayV2Api` 객체에는 Amazon API Gateway의 버전 2 API에 대한 정보가 들어 있습니다.

다음은 AWS Security Finding Format(ASFF)에서 `AwsApiGatewayV2Api` 조사 결과의 예제입니다. `AwsApiGatewayV2Api` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsApiGatewayV2ApiDetails 세부 정보를 참조하세요.

#### 예제

```
"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`에는 Amazon API Gateway의 버전 2 단계에 대한 정보가 들어 있습니다.

다음은 AWS Security Finding Format(ASFF)에서 `AwsApiGatewayV2Stage` 조사 결과의 예제입니다. `AwsApiGatewayV2Stage` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsApiGatewayV2StageDetails 세부 정보를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsAppSync 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi는 애플리케이션의 최상위 구성 요소인 an AWS AppSync GraphQL API에 대한 정보를 제공합니다.

다음 예제는 AwsAppSyncGraphQLApi 객체에 대한 ASFF를 보여 줍니다. AwsAppSyncGraphQLApi 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsAppSyncGraphQLApi 세부 정보를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsAthena 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsAthenaWorkGroup

AwsAthenaWorkGroup은(는) Amazon Athena 워크그룹에 대한 정보를 제공합니다. 워크그룹을 사용하면 사용자, 팀, 애플리케이션 또는 워크로드를 분리할 수 있습니다. 또한 데이터 처리 제한을 설정하고 비용을 추적하는 데도 도움이 됩니다.

다음 예제는 AwsAthenaWorkGroup 객체에 대한 ASFF를 보여 줍니다. AwsAthenaWorkGroup 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsAthenaWorkGroup 세부 정보를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsAutoScaling 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsAutoScalingAutoScalingGroup

`AwsAutoScalingAutoScalingGroup` 객체는 자동 스케일링 그룹에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding Format(ASFF)에서 `AwsAutoScalingAutoScalingGroup` 조사 결과의 예제입니다. `AwsAutoScalingAutoScalingGroup` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsAutoScalingAutoScalingGroupDetails 세부 정보를 참조하세요.

예제

```
"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

`AwsAutoScalingLaunchConfiguration` 객체는 시작 구성에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsAutoScalingLaunchConfiguration` 조사 결과 예입니다.

`AwsAutoScalingLaunchConfiguration` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsAutoScalingLaunchConfigurationDetails 세부 정보를 참조하세요.

예제

```
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 ASFF의 리소스

다음은 AwsBackup 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsBackupBackupPlan

AwsBackupBackupPlan 객체는 AWS Backup 백업 계획에 대한 정보를 제공합니다. AWS Backup 백업 계획은 AWS 리소스를 백업할 시기와 방법을 정의하는 정책 표현식입니다.

다음 예제에서는 AwsBackupBackupPlan 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsBackupBackupPlan 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsBackupBackupPlan 세부 정보를 참조하세요.

예제

```
"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

`AwsBackupBackupVault` 객체는 AWS Backup 백업 볼트에 대한 정보를 제공합니다. AWS Backup 백업 볼트는 백업을 저장하고 구성하는 컨테이너입니다.

다음 예제에서는 `AwsBackupBackupVault` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsBackupBackupVault` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsBackupBackupVault 세부 정보를 참조하세요.

#### 예제

```
"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

`AwsBackupRecoveryPoint` 객체는 복구 지점이라고도 하는 AWS Backup 백업에 대한 정보를 제공합니다. AWS Backup 복구 시점은 지정된 시간에 리소스의 콘텐츠를 나타냅니다.

다음 예제에서는 `AwsBackupRecoveryPoint` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsBackupBackupVault` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsBackupRecoveryPoint 세부 정보를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsCertificateManager` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsCertificateManagerCertificate

`AwsCertificateManagerCertificate` 객체는 AWS Certificate Manager (ACM) 인증서에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding Format(ASFF)의 `AwsCertificateManagerCertificate` 조사 결과 예입니다. `AwsCertificateManagerCertificate` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsCertificateManagerCertificateDetails 세부 정보를 참조하세요.

##### 예제

```
"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 ASFF의 리소스

다음은 `AwsCloudFormation` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsCloudFormationStack

`AwsCloudFormationStack` 객체는 최상위 템플릿에 리소스로 중첩된 AWS CloudFormation 스택에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsCloudFormationStack 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsCloudFormationStack 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsCloudFormationStackDetails 세부 정보를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsCloudFront 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsCloudFrontDistribution

`AwsCloudFrontDistribution` 객체는 Amazon CloudFront 배포 구성에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding Format(ASFF)에서 `AwsCloudFrontDistribution` 조사 결과의 예제입니다. `AwsCloudFrontDistribution` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsCloudFrontDistributionDetails 세부 정보를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsCloudTrail` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsCloudTrailTrail

`AwsCloudTrailTrail` 객체는 AWS CloudTrail 추적에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding Format(ASFF)에서 `AwsCloudTrailTrail` 조사 결과의 예제입니다. `AwsCloudTrailTrail` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsCloudTrailTrailDetails 세부 정보를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsCloudWatch` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsCloudWatchAlarm

`AwsCloudWatchAlarm` 객체는 경보 상태가 변경될 때 메트릭을 감시하거나 작업을 수행하는 Amazon CloudWatch 경보에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsCloudWatchAlarm` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsCloudWatchAlarm` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsCloudWatchAlarmDetails를 참조하세요.

#### 예제

```
"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 ASFF의 리소스

다음은 AwsCodeBuild 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsCodeBuildProject

AwsCodeBuildProject 객체는 AWS CodeBuild 프로젝트에 대한 정보를 제공합니다.

다음은 AWS Security Finding Format(ASFF)에서 AwsCodeBuildProject 조사 결과의 예제입니다. AwsCodeBuildProject 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsCodeBuildProjectDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsDms 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsDmsEndpoint

AwsDmsEndpoint 객체는 AWS Database Migration Service (AWS DMS) 엔드포인트에 대한 정보를 제공합니다. 엔드포인트는 데이터 저장소에 대한 연결, 데이터 저장소 유형, 위치 정보를 제공합니다.

다음 예제에서는 AwsDmsEndpoint 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsDmsEndpoint 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsDmsEndpointDetails를 참조하세요.

예제

```
"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

`AwsDmsReplicationInstance` 객체는 AWS Database Migration Service (AWS DMS) 복제 인스턴스에 대한 정보를 제공합니다. DMS는 복제 인스턴스를 사용하여 소스 데이터 저장소에 연결하고, 소스 데이터를 읽고, 대상 데이터 저장소에서 사용할 수 있도록 데이터 형식을 지정합니다.

다음 예제에서는 `AwsDmsReplicationInstance` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsDmsReplicationInstance` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsDmsReplicationInstanceDetails를 참조하세요.

예제

```
"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

`AwsDmsReplicationTask` 객체는 AWS Database Migration Service (AWS DMS) 복제 작업에 대한 정보를 제공합니다. 복제 작업은 소스 엔드포인트에서 대상 엔드포인트로 데이터 세트를 이동합니다.

다음 예제에서는 `AwsDmsReplicationInstance` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsDmsReplicationInstance` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsDmsReplicationInstance를 참조하세요.

## 예제


```
"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 ASFF의 리소스

다음은 AwsDynamoDB 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsDynamoDbTable

AwsDynamoDbTable 객체는 Amazon DynamoDB 테이블에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding Format(ASFF)에서 AwsDynamoDbTable 조사 결과의 예제입니다. AwsDynamoDbTable 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsDynamoDbTableDetails를 참조하세요.

##### 예제

```
"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 ASFF의 리소스

다음은 `AwsEc2` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsEc2ClientVpnEndpoint

`AwsEc2ClientVpnEndpoint` 객체는 AWS Client VPN 엔드포인트에 대한 정보를 제공합니다. Client VPN 엔드포인트는 클라이언트 VPN 세션을 활성화하고 관리하기 위해 생성 및 구성하는 리소스입니다. 이는 모든 Client VPN 세션의 종료 지점입니다.

다음 예제에서는 `AwsEc2ClientVpnEndpoint` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2ClientVpnEndpoint` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2ClientVpnEndpointDetails를 참조하세요.

#### 예제

```
"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

`AwsEc2Eip` 객체는 탄력적 IP 주소에 대한 정보를 제공합니다.

다음 예제에서는 `AwsEc2Eip` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2Eip` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2EipDetails를 참조하세요.

#### 예제

```
"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

`AwsEc2Instance` 객체는 Amazon EC2 인스턴스에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsEc2Instance 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEc2Instance 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2InstanceDetails를 참조하세요.

예제

```
"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

AwsEc2LaunchTemplate 객체에는 인스턴스 구성 정보를 지정하는 Amazon Elastic Compute Cloud 시작 템플릿에 대한 세부 정보가 들어 있습니다.

다음 예제에서는 AwsEc2LaunchTemplate 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEc2LaunchTemplate 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2LaunchTemplateDetails를 참조하세요.

예제

```
"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

`AwsEc2NetworkAcl` 객체에는 Amazon EC2 네트워크 액세스 제어 목록(ACL)에 대한 세부 정보가 포함됩니다.

다음 예제에서는 `AwsEc2NetworkAcl` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2NetworkAcl` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2NetworkAclDetails를 참조하세요.

예제

```
"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

`AwsEc2NetworkInterface` 객체는 Amazon EC2 네트워크 인터페이스에 대한 정보를 제공합니다.

다음 예제에서는 `AwsEc2NetworkInterface` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2NetworkInterface` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2NetworkInterfaceDetails를 참조하세요.

예제

```
"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

`AwsEc2RouteTable` 객체는 Amazon EC2 라우팅 테이블에 대한 정보를 제공합니다.

다음 예제에서는 `AwsEc2RouteTable` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2RouteTable` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2RouteTableDetails를 참조하세요.

#### 예제

```
"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

`AwsEc2SecurityGroup` 객체는 Amazon EC2 보안 그룹을 설명합니다.

다음 예제에서는 `AwsEc2SecurityGroup` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2SecurityGroup` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2SecurityGroupDetails를 참조하세요.

#### 예제

```
"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

`AwsEc2Subnet` 객체는 Amazon EC2의 서브넷에 대한 정보를 제공합니다.

다음 예제에서는 `AwsEc2Subnet` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2Subnet` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2SubnetDetails를 참조하세요.

예제

```
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

`AwsEc2TransitGateway` 객체는 Virtual Private Cloud(VPC)와 온프레미스 네트워크를 상호 연결하는 Amazon EC2 전송 게이트웨이에 대한 세부 정보를 제공합니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsEc2TransitGateway` 조사 결과 예입니다. `AwsEc2TransitGateway` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2TransitGatewayDetails를 참조하세요.

예제

```
"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

`AwsEc2Volume` 객체는 Amazon EC2 볼륨에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsEc2Volume` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2Volume` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2VolumeDetails를 참조하세요.

예제

```
"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

`AwsEc2Vpc` 객체는 Amazon EC2 VPC에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsEc2Vpc` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2Vpc` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2VpcDetails를 참조하세요.

예제

```
"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

`AwsEc2VpcEndpointService` 객체에는 VPC 엔드포인트 서비스의 서비스 구성에 대한 세부 정보가 들어 있습니다.

다음 예제에서는 `AwsEc2VpcEndpointService` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEc2VpcEndpointService` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2VpcEndpointServiceDetails를 참조하세요.

예제

```
"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

`AwsEc2VpcPeeringConnection` 객체는 두 VPC 간의 네트워킹 연결에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsEc2VpcPeeringConnection 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEc2VpcPeeringConnection 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEc2VpcPeeringConnectionDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsEcr 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsEcrContainerImage

AwsEcrContainerImage 객체는 Amazon ECR 이미지에 대한 정보를 제공합니다.

다음 예제에서는 AwsEcrContainerImage 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEcrContainerImage 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEcrContainerImageDetails를 참조하세요.

예제

```
"AwsEcrContainerImage": {
    "RegistryId": "123456789012",
    "RepositoryName": "repository-name",
    "Architecture": "amd64"
    "ImageDigest":
 "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
    "ImageTags": ["00000000-0000-0000-0000-000000000000"],
    "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

AwsEcrRepository 객체는 Amazon Elastic 컨테이너 레지스트리 리포지토리에 대한 정보를 제공합니다.

다음 예제에서는 AwsEcrRepository 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEcrRepository 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEcrRepositoryDetails를 참조하세요.

예제

```
"AwsEcrRepository": {
    "LifecyclePolicy": {
        "RegistryId": "123456789012",
    },
    "RepositoryName": "sample-repo",
    "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
    "ImageScanningConfiguration": {
        "ScanOnPush": true
    },
    "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs ASFF의 리소스

다음은 AwsEcs 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsEcsCluster

AwsEcsCluster 객체는 Amazon Elastic Container Service 클러스터에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsEcsCluster 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEcsCluster 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEcsClusterDetails를 참조하세요.

예제

```
    "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

`AwsEcsContainer` 객체에는 Amazon ECS 컨테이너에 대한 세부 정보가 들어 있습니다.

다음 예제에서는 `AwsEcsContainer` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEcsContainer` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEcsContainerDetails를 참조하세요.

#### 예제

```
"AwsEcsContainer": {
    "Image": "1111111/
knotejs@sha256:356131c9fef111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
        "ContainerPath": "/mnt/etc",
        "SourceVolume": "vol-03909e9"
    }],
    "Name": "knote",
    "Privileged": true
}
```

### AwsEcsService

`AwsEcsService` 객체는 Amazon ECS 클러스터 내의 서비스에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsEcsService` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEcsService` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEcsServiceDetails를 참조하세요.

예제

```
"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

AwsEcsTask 객체는 Amazon ECS 작업에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsEcsTask 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEcsTask 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEcsTask를 참조하세요.

예제

```
"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

AwsEcsTaskDefinition 객체에는 작업 정의에 대한 세부 정보가 들어 있습니다. 작업 정의는 Amazon Elastic Container Service 작업의 컨테이너 및 볼륨 정의를 설명합니다.

다음 예제에서는 AwsEcsTaskDefinition 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEcsTaskDefinition 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEcsTaskDefinitionDetails를 참조하세요.

예제

```
    "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 ASFF의 리소스

다음은 AwsEfs 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsEfsAccessPoint

AwsEfsAccessPoint 객체는 Amazon Elastic File System에 저장된 파일에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsEfsAccessPoint 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEfsAccessPoint 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEfsAccessPointDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsEks` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsEksCluster

`AwsEksCluster` 객체는 Amazon EKS 클러스터에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsEksCluster` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEksCluster` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEksClusterDetails를 참조하세요.

#### 예제

```
{
  "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 ASFF의 리소스

다음은 AwsElasticBeanstalk 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsElasticBeanstalkEnvironment

AwsElasticBeanstalkEnvironment 개체에는 AWS Elastic Beanstalk 환경에 대한 세부 정보가 들어 있습니다.

다음 예제에서는 AwsElasticBeanstalkEnvironment 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsElasticBeanstalkEnvironment 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsElasticBeanstalkEnvironmentDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsElasticSearch` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsElasticSearchDomain

`AwsElasticSearchDomain` 객체는 Amazon OpenSearch Service 도메인에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsElasticSearchDomain` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsElasticSearchDomain` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsElasticSearchDomainDetails를 참조하세요.

#### 예제

```
"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 ASFF의 리소스

다음은 `AwsElb` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsElbLoadBalancer

`AwsElbLoadBalancer` 객체에는 Classic Load Balancer에 대한 세부 정보가 포함됩니다.

다음 예제에서는 `AwsElbLoadBalancer` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsElbLoadBalancer` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsElbLoadBalancerDetails를 참조하세요.

#### 예제

```
"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

`AwsElbv2LoadBalancer` 객체는 로드 밸런서에 대한 정보를 제공합니다.

다음 예제에서는 `AwsElbv2LoadBalancer` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsElbv2LoadBalancer` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsElbv2LoadBalancerDetails를 참조하세요.

#### 예제

```
"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 ASFF의 리소스

다음은 `AwsEventBridge` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsEventSchemasRegistry

`AwsEventSchemasRegistry` 객체는 Amazon EventBridge 스키마 레지스트리에 대한 정보를 제공합니다. 스키마는 EventBridge로 보내는 이벤트의 구조를 정의합니다. 스키마 레지스터는 스키마를 수집하고 논리적으로 그룹화하는 컨테이너입니다.

다음 예제에서는 `AwsEventSchemasRegistry` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsEventSchemasRegistry` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEventSchemasRegistry를 참조하세요.

예제

```
"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}
```

AwsEventsEndpoint

`AwsEventsEndpoint` 객체는 Amazon EventBridge 글로벌 엔드포인트에 대한 정보를 제공합니다. 엔드포인트는 리전 내결함성을 높여 애플리케이션의 가용성을 향상시킬 수 있습니다.

다음 예제에서는 AwsEventsEndpoint 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEventsEndpoint 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEventsEndpointDetails를 참조하세요.

예제

```
"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

AwsEventsEventbus 객체는 Amazon EventBridge 글로벌 엔드포인트에 대한 정보를 제공합니다. 엔드포인트는 리전 내결함성을 높여 애플리케이션의 가용성을 향상시킬 수 있습니다.

다음 예제에서는 AwsEventsEventbus 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsEventsEventbus 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsEventsEventbusDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsGuardDuty 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsGuardDutyDetector

AwsGuardDutyDetector 객체는 Amazon GuardDuty 감지기에 대한 정보를 제공합니다. 감지기는 GuardDuty 서비스를 나타내는 객체입니다. 감지기는 GuardDuty가 작동하는 데 필요합니다.

다음 예제에서는 AwsGuardDutyDetector 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsGuardDutyDetector 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsGuardDutyDetector를 참조하세요.

예제

```
"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"
         }
    }
}
```

### AwsIam ASFF의 리소스

다음은 `AwsIam` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsIamAccessKey

`AwsIamAccessKey` 객체에는 조사 결과와 관련된 IAM 액세스 키에 대한 세부 정보가 들어 있습니다.

다음 예제에서는 AwsIamAccessKey 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsIamAccessKey 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsIamAccessKeyDetails를 참조하세요.

예제

```
"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

AwsIamGroup 객체에는 IAM 그룹에 대한 세부 정보가 포함됩니다.

다음 예제에서는 AwsIamGroup 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsIamGroup 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsIamGroupDetails를 참조하세요.

예제

```
"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

`AwsIamPolicy` 객체는 IAM 권한 정책을 나타냅니다.

다음 예제에서는 `AwsIamPolicy` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsIamPolicy` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsIamPolicyDetails를 참조하세요.

#### 예제

```
"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

`AwsIamRole` 객체는 역할의 정책을 모두 포함한 IAM 역할에 대한 정보가 들어 있습니다.

다음 예제에서는 `AwsIamRole` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsIamRole` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsIamRoleDetails를 참조하세요.

예제

```
"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

`AwsIamUser` 객체는 사용자에 대한 정보를 제공합니다.

다음 예제에서는 `AwsIamUser` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsIamUser` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsIamUserDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsKinesis` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsKinesisStream

`AwsKinesisStream` 객체는 Amazon Kinesis Data Streams에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsKinesisStream` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsKinesisStream` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsKinesisStreamDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsKms` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsKmsKey

`AwsKmsKey` 객체는에 대한 세부 정보를 제공합니다 AWS KMS key.

다음 예제에서는 AwsKmsKey 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsKmsKey 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsKmsKeyDetails를 참조하세요.

예제

```
"AwsKmsKey": {
                        "AWSAccountId": "string",
                        "CreationDate": "string",
                        "Description": "string",
                        "KeyId": "string",
                        "KeyManager": "string",
                        "KeyRotationStatus": boolean,
                        "KeyState": "string",
                        "Origin": "string"
                    }
```

AwsLambda

다음은 AwsLambda 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsLambdaFunction

AwsLambdaFunction 객체는 Lambda 함수의 구성에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsLambdaFunction 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsLambdaFunction 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsLambdaFunctionDetails를 참조하세요.

예제

```
"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

`AwsLambdaLayerVersion` 객체는 Lambda 계층 버전에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsLambdaLayerVersion 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsLambdaLayerVersion 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsLambdaLayerVersionDetails를 참조하세요.

예제

```
"AwsLambdaLayerVersion": {
    "Version": 2,
    "CompatibleRuntimes": [
        "java8"
    ],
    "CreatedDate": "2019-10-09T22:02:00.274+0000"
}
```

AwsMsk ASFF의 리소스

다음은 AwsMsk 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsMskCluster

이 AwsMskCluster 객체는 Amazon Managed Streaming for Apache Kafka(Amazon MSK) 클러스터에 대한 정보를 제공합니다.

다음 예제에서는 AwsMskCluster 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsMskCluster 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsMskClusterDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsNetworkFirewall` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsNetworkFirewallFirewall

`AwsNetworkFirewallFirewall` 객체에는 AWS Network Firewall 방화벽에 대한 세부 정보가 포함됩니다.

다음 예제에서는 `AwsNetworkFirewallFirewall` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsNetworkFirewallFirewall` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsNetworkFirewallFirewallDetails를 참조하세요.

예제

```
"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

`AwsNetworkFirewallFirewallPolicy` 객체는 방화벽 정책에 대한 세부 정보를 제공합니다. 방화벽 정책은 네트워크 방화벽의 동작을 정의합니다.

다음 예제에서는 `AwsNetworkFirewallFirewallPolicy` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsNetworkFirewallFirewallPolicy` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsNetworkFirewallFirewallPolicyDetails를 참조하세요.

예제

```
"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

AwsNetworkFirewallRuleGroup 객체는 AWS Network Firewall 규칙 그룹에 대한 세부 정보를 제공합니다. 규칙 그룹은 네트워크 트래픽을 검사하고 제어하는 데 사용됩니다. 상태 비저장 규칙 그룹은 개별 패킷에 적용됩니다. 상태 저장 규칙 그룹은 트래픽 흐름의 컨텍스트에서 패킷에 적용됩니다.

규칙 그룹은 방화벽 정책에서 참조됩니다.

다음 예제에서는 AwsNetworkFirewallRuleGroup 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsNetworkFirewallRuleGroup 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsNetworkFirewallRuleGroupDetails를 참조하세요.

예제 - 상태 비저장 규칙 그룹

```
"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"
                                    }
                                ]
                            }
                        }
                    }
                ]
            }
        }
    }
}
```

## 예제 - 상태 저장 규칙 그룹

```
"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"
                        }
                    ]
                }
            ]
         }
    }
}
```

다음은 AwsNetworkFirewallRuleGroup 속성에 대한 유효한 값 예제 목록입니다.

- Action

  유효한 값: PASS | DROP | ALERT

- Protocol

  유효한 값: IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- Flags

유효한 값: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- Masks

  유효한 값: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

### AwsOpenSearchService ASFF의 리소스

다음은 AwsOpenSearchService 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

#### AwsOpenSearchServiceDomain

AwsOpenSearchServiceDomain 객체에는 Amazon OpenSearch Service 도메인에 대한 정보가 들어 있습니다.

다음 예제에서는 AwsOpenSearchServiceDomain 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsOpenSearchServiceDomain 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsOpenSearchServiceDomainDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsRds 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsRdsDbCluster

AwsRdsDbCluster 객체는 Amazon RDS 데이터베이스 클러스터에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsRdsDbCluster 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsRdsDbCluster 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRdsDbClusterDetails를 참조하세요.

예제

```
"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

`AwsRdsDbClusterSnapshot` 객체에는 Amazon RDS DB 클러스터 스냅샷에 대한 정보가 포함됩니다.

다음 예제에서는 `AwsRdsDbClusterSnapshot` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsRdsDbClusterSnapshot` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRdsDbClusterSnapshotDetails를 참조하세요.

#### 예제

```
"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

`AwsRdsDbInstance` 객체는 Amazon RDS DB 인스턴스에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsRdsDbInstance` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsRdsDbInstance` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRdsDbInstanceDetails를 참조하세요.

#### 예제

```
"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

`AwsRdsDbSecurityGroup` 객체에는 Amazon Relational Database Service에 대한 정보가 포함됩니다.

다음 예제에서는 `AwsRdsDbSecurityGroup` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsRdsDbSecurityGroup` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRdsDbSecurityGroupDetails를 참조하세요.

#### 예제

```
"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

AwsRdsDbSnapshot 객체에는 Amazon RDS DB 클러스터 스냅샷에 대한 세부 정보가 포함됩니다.

다음 예제에서는 AwsRdsDbSnapshot 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsRdsDbSnapshot 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRdsDbSnapshotDetails를 참조하세요.

#### 예제

```
"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

`AwsRdsEventSubscription`에는 RDS 이벤트 알림 구독에 대한 세부 정보가 들어 있습니다. 구독을 통해 RDS는 SNS 주제에 이벤트를 게시할 수 있습니다.

다음 예제에서는 `AwsRdsEventSubscription` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsRdsEventSubscription` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRdsEventSubscriptionDetails를 참조하세요.

#### 예제

```
"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 ASFF의 리소스

다음은 `AwsRedshift` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsRedshiftCluster

`AwsRedshiftCluster` 객체에는 Amazon Redshift 클러스터에 대한 세부 정보가 포함됩니다.

다음 예제에서는 `AwsRedshiftCluster` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsRedshiftCluster` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRedshiftClusterDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsRoute53 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsRoute53HostedZone

AwsRoute53HostedZone객체는 호스팅 영역에 할당된 4개의 이름 서버를 포함하여 Amazon Route 53 호스팅 영역에 대한 정보를 제공합니다. 호스팅 영역은 단일 상위 도메인 이름에 속하는 함께 관리할 수 있는 기록 컬렉션을 나타냅니다.

다음 예제에서는 AwsRoute53HostedZone 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsRoute53HostedZone 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsRoute53HostedZoneDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsS3 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsS3AccessPoint

AwsS3AccessPoint는 Amazon S3 Access Points에 대한 정보를 제공합니다. S3 액세스 포인트는 S3 객체 작업을 수행하는 데 사용할 수 있는 S3 버킷에 연결된 네트워크 엔드포인트입니다.

다음 예제에서는 AwsS3AccessPoint 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsS3AccessPoint 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsS3AccessPointDetails를 참조하세요.

예제

```
"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

AwsS3AccountPublicAccessBlock은(는) 계정의 Amazon S3 퍼블릭 액세스 차단 구성에 대한 정보를 제공합니다.

다음 예제에서는 AwsS3AccountPublicAccessBlock 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsS3AccountPublicAccessBlock 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsS3AccountPublicAccessBlockDetails를 참조하세요.

예제

```
"AwsS3AccountPublicAccessBlock": {
    "BlockPublicAcls": true,
    "BlockPublicPolicy": true,
    "IgnorePublicAcls": false,
    "RestrictPublicBuckets": true
}
```

### AwsS3Bucket

`AwsS3Bucket` 객체는 Amazon S3 버킷에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsS3Bucket` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsS3Bucket` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsS3BucketDetails를 참조하세요.

예제


```
"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"
                }
            }
        ]
     }
}
```

AwsS3Object

`AwsS3Object` 객체는 Amazon S3 객체에 대한 정보를 제공합니다.

다음 예제에서는 `AwsS3Object` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsS3Object` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsS3ObjectDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsSageMaker` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsSageMakerNotebookInstance

`AwsSageMakerNotebookInstance` 객체는 Jupyter Notebook 앱을 실행하는 기계 학습 컴퓨팅 인스턴스인 Amazon SageMaker AI 노트북 인스턴스에 대한 정보를 제공합니다.

다음 예제에서는 `AwsSageMakerNotebookInstance` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsSageMakerNotebookInstance` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsSageMakerNotebookInstanceDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsSecretsManager` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsSecretsManagerSecret

이 AwsSecretsManagerSecret 객체는 Secrets Manager 암호에 대한 세부 정보를 제공합니다.

다음 예제에서는 AwsSecretsManagerSecret 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsSecretsManagerSecret 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsSecretsManagerSecretDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsSns 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsSnsTopic

AwsSnsTopic 객체에는 Amazon Simple Notification Service 주제에 대한 세부 정보가 포함됩니다.

다음 예제에서는 AwsSnsTopic 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsSnsTopic 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsSnsTopicDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 AwsSqs 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

### AwsSqsQueue

AwsSqsQueue 객체에는 Amazon Simple Queue Service 대기열에 대한 정보가 들어 있습니다.

다음 예제에서는 AwsSqsQueue 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsSqsQueue 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsSqsQueueDetails를 참조하세요.

#### 예제

```
"AwsSqsQueue": {
    "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
```

```
    "KmsDataKeyReusePeriodSeconds": 60,,
    "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
    "QueueName": "sample-queue"
}
```

AwsSsm ASFF의 리소스

다음은 AwsSsm 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsSsmPatchCompliance

AwsSsmPatchCompliance 객체는 인스턴스를 패치하는 데 사용된 패치 기준선을 기반으로 인스턴스의 패치 상태에 대한 정보를 제공합니다.

다음 예제에서는 AwsSsmPatchCompliance 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsSsmPatchCompliance 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsSsmPatchComplianceDetails를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsStepFunctions` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsStepFunctionStateMachine

`AwsStepFunctionStateMachine` 객체는 일련의 이벤트 기반 단계로 구성된 워크플로인 AWS Step Functions 상태 시스템에 대한 정보를 제공합니다.

다음 예제에서는 `AwsStepFunctionStateMachine` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsStepFunctionStateMachine` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsStepFunctionStateMachine를 참조하세요.

예제

```
"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 ASFF의 리소스

다음은 `AwsWaf` 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsWafRateBasedRule

AwsWafRateBasedRule 객체에는 글로벌 리소스의 AWS WAF 속도 기반 규칙에 대한 세부 정보가 들어 있습니다. AWS WAF 속도 기반 규칙은 요청을 허용, 차단 또는 계산할 시기를 나타내는 설정을 제공합니다. 속도 기반 규칙은 지정된 기간 동안 도착한 요청 수를 포함합니다.

다음 예제에서는 AwsWafRateBasedRule 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsWafRateBasedRule 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafRateBasedRuleDetails를 참조하세요.

예제

```
"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

AwsWafRegionalRateBasedRule 객체에는 리전 리소스의 속도 기반 규칙에 대한 세부 정보가 들어 있습니다. 속도 기반 규칙은 요청을 허용, 차단 또는 계산할 시기를 지정하는 설정을 제공합니다. 속도 기반 규칙은 지정된 기간 동안 도착한 요청 수를 포함합니다.

다음 예제에서는 AwsWafRegionalRateBasedRule 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsWafRegionalRateBasedRule 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafRegionalRateBasedRuleDetails를 참조하세요.

예제

```
"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

`AwsWafRegionalRule` 객체는 AWS WAF 리전 규칙에 대한 세부 정보를 제공합니다. 이 규칙은 허용, 차단 또는 계산하려는 웹 요청을 식별합니다.

다음 예제에서는 `AwsWafRegionalRule` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsWafRegionalRule` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafRegionalRuleDetails를 참조하세요.

예제

```
"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

`AwsWafRegionalRuleGroup` 객체는 AWS WAF 리전 규칙 그룹에 대한 세부 정보를 제공합니다. 규칙 그룹은 웹 액세스 제어 목록(웹 ACL)에 추가하는 사전 정의된 규칙 모음입니다.

다음 예제에서는 `AwsWafRegionalRuleGroup` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsWafRegionalRuleGroup` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafRegionalRuleGroupDetails를 참조하세요.

예제

```
"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`는 AWS WAF 리전별 웹 액세스 제어 목록(웹 ACL)에 대한 세부 정보를 제공합니다. 웹 ACL에는 허용, 차단 또는 계산할 요청을 식별하는 규칙이 포함되어 있습니다.

다음은 AWS Security Finding Format(ASFF)에서 `AwsWafRegionalWebAcl` 조사 결과의 예제입니다. `AwsApiGatewayV2Stage` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafRegionalWebAclDetails를 참조하세요.

#### 예제

```
"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`는 AWS WAF 규칙에 대한 정보를 제공합니다. AWS WAF 규칙은 허용, 차단 또는 계산하려는 웹 요청을 식별합니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsWafRule` 조사 결과 예입니다. `AwsApiGatewayV2Stage` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafRuleDetails를 참조하세요.

예제

```
"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`는 AWS WAF 규칙 그룹에 대한 정보를 제공합니다. AWS WAF 규칙 그룹은 웹 액세스 제어 목록(웹 ACL)에 추가하는 미리 정의된 규칙의 모음입니다.

다음은 AWS Security Finding 형식(ASFF)의 `AwsWafRuleGroup` 조사 결과 예제입니다. `AwsApiGatewayV2Stage` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafRuleGroupDetails를 참조하세요.

예제

```
"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

`AwsWafv2RuleGroup` 객체는 AWS WAF V2 규칙 그룹에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsWafv2RuleGroup` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsWafv2RuleGroup` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafv2RuleGroupDetails를 참조하세요.

#### 예제

```
"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

`AwsWafWebAcl` 객체는 AWS WAF 웹 ACL에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsWafWebAcl` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsWafWebAcl` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafWebAclDetails를 참조하세요.

예제

```
"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

`AwsWafv2WebAcl` 객체는 AWS WAF V2 웹 ACL에 대한 세부 정보를 제공합니다.

다음 예제에서는 `AwsWafv2WebAcl` 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. `AwsWafv2WebAcl` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsWafv2WebAclDetails를 참조하세요.

#### 예제

```
"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 ASFF의 리소스

다음은 AwsXray 리소스에 대한 AWS Security Finding Format(ASFF) 구문의 예입니다.

AWS Security Hub CSPM 는 다양한 소스의 결과를 ASFF로 정규화합니다. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

AwsXrayEncryptionConfig

AwsXrayEncryptionConfig 객체에는의 암호화 구성에 대한 정보가 포함되어 있습니다 AWS X-Ray.

다음 예제에서는 AwsXrayEncryptionConfig 객체의 AWS Security Finding Format(ASFF)을 보여줍니다. AwsXrayEncryptionConfig 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 AwsXrayEncryptionConfigDetails를 참조하세요.

예제

```
"AwsXRayEncryptionConfig":{
    "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",
    "Status": "UPDATING",
    "Type":"KMS"
}
```

ASFF의 CodeRepository 객체

CodeRepository 객체는 AWS 리소스에 연결하고 취약성을 검사하도록 Amazon Inspector를 구성한 외부 코드 리포지토리에 대한 정보를 제공합니다.

다음 예제에서는 CodeRepository 객체에 대한 AWS Security Finding Format(ASFF) 구문을 보여줍니다. CodeRepository 속성에 대한 설명을 보려면 AWS Security Hub API 참조의

CodeRepositoryDetails를 참조하세요. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

예제

```
"CodeRepository": {
    "ProviderType": "GITLAB_SELF_MANAGED",
    "ProjectName": "projectName",
    "CodeSecurityIntegrationArn": "arn:aws:inspector2:us-
east-1:123456789012:codesecurity-integration/00000000-0000-0000-0000-000000000000"
}
```

### ASFF의 Container 객체

다음 예제에서는 `Container` 객체에 대한 AWS Security Finding Format(ASFF) 구문을 보여줍니다. `Container` 속성에 대한 설명을 보려면 AWS Security Hub API 참조의 ContainerDetails를 참조하세요. ASFF에 대한 배경 정보는 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

예제

```
"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"
    }]
}
```

### ASFF의 Other 객체

AWS Security Finding Format(ASFF)에서 `Other` 객체는 사용자 지정 필드와 값을 지정합니다. ASFF에 대한 자세한 내용은 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

`Other` 객체를 사용하여 리소스에 대한 사용자 지정 필드 및 값을 지정할 수 있습니다. 다음과 같은 경우 `Other` 객체를 사용할 수 있습니다.

- 리소스 유형에 해당 `Details` 객체가 없습니다. 리소스에 대한 세부 정보를 지정하려면 `Other` 객체를 사용합니다.
- 리소스 유형에 대한 `Details` 객체에는 지정하려는 속성이 모두 포함되어 있지 않습니다. 이 경우, 리소스 유형에 대한 `Details` 객체를 사용하여 사용 가능한 필드를 지정합니다. `Other` 객체를 사용하여 유형별 `Details` 객체에 없는 속성을 지정할 수 있습니다.
- 리소스 유형이 제공된 유형 중 하나가 아닙니다. 이 경우, `Resource.Type`을 `Other`로 설정하고 `Other` 객체를 사용하여 세부 정보를 지정합니다.

유형: 최대 50개의 키-값 쌍의 맵

각 키-값 쌍은 다음 요구 사항을 충족해야 합니다.

- 키는 128자 미만이어야 합니다.
- 값은 1,024자 미만이어야 합니다.

# Security Hub CSPM에서 인사이트 보기

AWSSecurity Hub CSPM에서 인사이트는 관련 조사 결과의 모음입니다. 인사이트는 주의와 개입이 필요한 보안 영역을 식별합니다. 예를 들어, 인사이트는 잘못된 보안 관행을 감지하는 조사 결과의 대상이 되는 EC2 인스턴스를 지정할 수 있습니다. 인사이트는 전체 조사 결과 공급자의 조사 결과를 함께 나타냅니다.

각 인사이트는 그룹화 기준 문과 선택적 필터에 의해 정의됩니다. 그룹화 기준 문은 일치하는 조사 결과를 그룹화하는 방법을 나타내며 인사이트가 적용되는 항목 유형을 식별합니다. 예를 들어, 인사이트가 리소스 식별자별로 그룹화된 경우, 인사이트는 리소스 식별자 목록을 생성합니다. 선택적 필터는 인사이트와 일치하는 조사 결과의 범위를 식별합니다. 예를 들어, 특정 공급자의 조사 결과나 특정 리소스 유형과 연관된 조사 결과만 볼 수 있습니다.

Security Hub CSPM에서는 여러 가지 기본 제공 관리형 인사이트를 제공합니다. 관리형 인사이트는 수정하거나 삭제할 수 없습니다. AWS환경 및 사용량에 고유한 보안 문제를 추적하려면 사용자 지정 인사이트를 생성할 수 있습니다.

AWSSecurity Hub CSPM 콘솔의 인사이트 페이지에는 사용 가능한 인사이트 목록이 표시됩니다.

기본적으로 목록에는 관리형 인사이트와 사용자 지정 인사이트가 모두 표시됩니다. 인사이트 유형을 기반으로 인사이트 목록을 필터링하려면 필터 필드 옆에 있는 드롭다운 메뉴에서 인사이트 유형을 선택합니다.

- 사용 가능한 인사이트를 모두 표시하려면 모든 인사이트를 선택합니다. 이 항목이 기본 옵션입니다.
- 관리형 인사이트만 표시하려면 Security Hub CSPM 관리형 인사이트를 선택합니다.
- 사용자 지정 인사이트만 표시하려면 사용자 지정 인사이트를 선택합니다.

또한, 인사이트 이름을 기반으로 인사이트 목록을 필터링할 수 있습니다. 이렇게 하려면 필터 필드에서 목록을 필터링하는 데 사용할 텍스트를 입력합니다. 필터는 대소문자를 구분하지 않습니다. 필터는 인사이트 이름의 모든 위치에서 텍스트가 포함된 인사이트를 찾습니다.

인사이트는 일치하는 조사 결과를 생성하는 통합 또는 표준을 활성화한 경우에만 결과를 반환합니다. 예를 들어, 관리형 인사이트 29. 실패한 CIS 점검 횟수별 상위 리소스는 인터넷 보안 센터(CIS) AWS Foundations Benchmark 표준의 한 버전을 활성화한 경우에만 결과를 반환합니다.

## Security Hub CSPM에서 인사이트 검토 및 조치

각 인사이트에 대해 AWS Security Hub CSPM은 먼저 필터 기준과 일치하는 결과를 확인한 다음 그룹화 속성을 사용하여 일치하는 결과를 그룹화합니다.

콘솔의 인사이트 페이지에서 결과 및 조사 결과를 보고 조치를 취할 수 있습니다.

교차 리전 집계를 활성화하면, 관리형 인사이트 조사 결과(집계 리전에 로그인한 경우)에 집계 리전 및 연결된 리전에서 나온 조사 결과가 포함됩니다. 사용자 지정 인사이트 조사 결과의 경우 또한, 인사이트가 리전별로 필터링되지 않으면 집계 리전 및 연결된 리전의 조사 결과가 조사 결과에 포함됩니다(집계 리전에 로그인한 경우). 다른 리전에는 인사이트 결과가 해당 리전에 대한 것만 해당됩니다.

교차 리전 집계에 대한 자세한 내용은 the section called “리전 간 데이터 집계” 섹션을 참조하세요.

### 인사이트 결과 보기 및 조치 수행

인사이트 결과는 인사이트에 대한 결과의 그룹화된 목록으로 구성됩니다. 예를 들어, 인사이트가 리소스 ID별로 그룹화된 경우, 인사이트 결과는 리소스 ID의 목록입니다. 조사 결과 목록의 각 항목은 해당 항목에 일치하는 조사 결과 수를 나타냅니다.

조사 결과를 리소스 식별자 또는 리소스 유형으로 그룹화하는 경우, 조사 결과에는 일치하는 조사 결과에 있는 모든 리소스가 포함됩니다. 여기에는 필터 기준의 리소스 유형과 유형이 다른 리소스가 포함됩니다. 예를 들어, 인사이트 는 S3 버킷과 관련된 조사 결과를 식별합니다. 일치하는 조사 결과에 S3 버킷 리소스와 IAM 액세스 키 리소스가 모두 포함된 경우, 인사이트 조사 결과에는 두 리소스가 모두 포함됩니다.

Security Hub CSPM 콘솔에서 조사 결과 목록은 가장 적게 일치하는 조사 결과부터 순서대로 정렬됩니다. Security Hub CSPM은 결과를 100개만 표시할 수 있습니다. 그룹화 값이 100개를 초과하는 경우, 처음 100개만 표시됩니다.

조사 결과 목록 외에도 인사이트 조사 결과에는 다음 속성에 대해 일치하는 조사 결과 수를 요약하는 차트 세트가 표시됩니다.

- 심각도 레이블 - 각 심각도 레이블에 대한 조사 결과 수
- AWS 계정 ID - 일치하는 조사 결과에 대한 상위 5IDs
- 리소스 유형 - 일치하는 조사 결과에 대한 상위 5개 리소스 유형
- 리소스 ID - 일치하는 조사 결과에 대한 상위 5개 리소스 ID
- 제품 이름 - 일치하는 조사 결과에 대한 상위 5개 조사 결과 공급자

사용자 지정 작업을 구성한 경우, 선택한 결과를 사용자 지정 작업으로 보낼 수 있습니다. 이 작업은 `Security Hub Insight Results` 이벤트 유형에 대한 Amazon CloudWatch 규칙과 연결되어야 합니다. 자세한 내용은 the section called “자동 응답 및 해결” 섹션을 참조하세요. 사용자 지정 작업을 구성하지 않으면 작업 메뉴가 비활성화됩니다.

Security Hub CSPM console

인사이트 결과 보기 및 조치 수행(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 인사이트 결과 목록을 표시하려면 인사이트 이름을 선택합니다.
4. 사용자 지정 작업으로 보낼 각 결과에 대한 확인란을 선택합니다.
5. 작업 메뉴에서 사용자 지정 작업을 선택합니다.

Security Hub CSPM API, AWS CLI

인사이트 결과를 보고 이에 대한 조치를 취하려면(API, AWS CLI)

인사이트 결과를 보려면 Security Hub CSPM API의 >GetInsightResults 작업을 사용합니다. 를 사용하는 경우 get-insight-results 명령을 AWS CLI실행합니다.

결과를 반환할 인사이트를 식별하려면 인사이트 ARN이 필요합니다. 사용자 지정 인사이트를 위한 인사이트 ARN을 얻으려면 `GetInsights` 작업이나 get-insight-results 명령을 사용합니다.

다음 예제에서는 지정된 인사이트에 대한 결과를 검색합니다. 이 예제는 Linux, macOS 또는 Unix 용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

프로그래밍 방식으로 사용자 지정 작업을 생성하는 방법에 대한 자세한 내용은 사용자 지정 작업을 사용하여 조사 결과 및 인사이트 조사 결과를 EventBridge로 전송 섹션을 참조하세요.

### 인사이트 조사 결과에 대한 보기 및 조치 수행(콘솔)

Security Hub CSPM 콘솔의 인사이트 조사 결과 목록에서 각 조사 결과에 대한 조사 결과 목록을 표시할 수 있습니다.

인사이트 조사 결과를 표시하고 조치를 취하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 인사이트 결과 목록을 표시하려면 인사이트 이름을 선택합니다.
4. 인사이트 조사 결과에 대한 조사 결과 목록을 표시하려면 조사 결과 목록에서 항목을 선택합니다. 조사 결과 목록에는 워크플로우 상태가 `NEW` 또는 `NOTIFIED`인 선택한 통합에 대한 활성 조사 결과가 표시됩니다.

조사 결과 목록에서 다음 작업을 수행할 수 있습니다.

- Security Hub CSPM에서 조사 결과 필터링
- 조사 결과 세부 정보 및 기록 검토
- Security Hub CSPM에서 조사 결과의 워크플로 상태 설정
- 사용자 지정 Security Hub CSPM 작업으로 조사 결과 전송

## Security Hub CSPM의 관리형 인사이트

AWSSecurity Hub CSPM은 여러 관리형 인사이트를 제공합니다.

Security Hub CSPM 관리형 인사이트는 편집하거나 삭제할 수 없습니다. 인사이트 조사 결과와 조사 결과를 보고 조치를 취할 수 있습니다. 관리형 인사이트를 새로운 사용자 지정 인사이트의 기반으로 사용할 수도 있습니다.

다른 모든 인사이트과 마찬가지로, 관리형 인사이트는 일치하는 조사 결과를 생성할 수 있는 제품 통합 또는 보안 표준을 활성화한 경우에만 조사 결과를 반환합니다.

리소스 식별자별로 그룹화된 인사이트의 경우, 조사 결과에는 일치하는 조사 결과에 있는 모든 리소스의 식별자가 포함됩니다. 여기에는 필터 기준의 리소스 유형과 유형이 다른 리소스가 포함됩니다. 예를 들어, 다음 목록에 있는 인사이트 2는 Amazon S3 버킷과 관련된 조사 결과를 식별합니다. 일치하는 조사 결과에 S3 버킷 리소스와 IAM 액세스 키 리소스가 모두 포함된 경우, 인사이트 조사 결과에는 두 리소스가 모두 포함됩니다.

Security Hub CSPM은 현재 다음과 같은 관리형 인사이트를 제공합니다.

1. 결과가 가장 많은 AWS리소스

   ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

   그룹화 기준: 리소스 식별자

   조사 결과 필터:
   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임
2. 퍼블릭 쓰기 또는 읽기 권한이 있는 S3 버킷

   ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

   그룹화 기준: 리소스 식별자

   조사 결과 필터:
   - 유형이 `Effects/Data Exposure`로 시작
   - 리소스 유형이 `AwsS3Bucket`임
   - 레코드 상태가 `ACTIVE`임
   - 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임
3. 가장 많은 조사 결과를 생성하는 AMI

   ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

   그룹화 기준: EC2 인스턴스 이미지 ID

조사 결과 필터:

- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

4. 알려진 Tactics, Techniques, and Procedures(TTP)와 관련된 EC2 인스턴스

ARN: arn:aws:securityhub:::insight/securityhub/default/14

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 TTPs로 시작
- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

5. 의심스러운 액세스 키 활동이 있는 보안 AWS주체

ARN: arn:aws:securityhub:::insight/securityhub/default/9

그룹화 기준: IAM 액세스 키 보안 주체 이름

조사 결과 필터:

- 리소스 유형이 AwsIamAccessKey임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

6.보안 표준/모범 사례를 충족하지 않는 인스턴스AWS를 리소스합니다.

ARN: arn:aws:securityhub:::insight/securityhub/default/6

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

7. 잠재적 데이터 유출과 관련된 AWS리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/7

그룹화 기준:: 리소스 ID

조사 결과 필터:

- 유형이 Effects/Data Exfiltration/로 시작
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

8.무단 AWS리소스 소비와 관련된 리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/8

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 Effects/Resource Consumption로 시작
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

9. 보안 표준/모범 사례를 준수하지 않는 S3 버킷

ARN: arn:aws:securityhub:::insight/securityhub/default/11

그룹화 기준: 리소스 ID

조사 결과 필터:

- 리소스 유형이 AwsS3Bucket임
- 유형이 Software and Configuration Checks/Industry and Regulatory Standards/AWSSecurity Best Practices임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

10. 민감한 데이터가 포함된 S3 버킷

ARN: arn:aws:securityhub:::insight/securityhub/default/12

그룹화 기준: 리소스 ID

조사 결과 필터:

- 리소스 유형이 AwsS3Bucket임
- 유형이 Sensitive Data Identifications/로 시작
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

11. 유출되었을 수 있는 자격 증명

    ARN: arn:aws:securityhub:::insight/securityhub/default/13

    그룹화 기준: 리소스 ID

    조사 결과 필터:

- 유형이 Sensitive Data Identifications/Passwords/로 시작
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

12. 중요한 취약성에 대한 보안 패치가 없는 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/16

    그룹화 기준: 리소스 ID

    조사 결과 필터:

- 유형이 Software and Configuration Checks/Vulnerabilities/CVE로 시작
- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

13. 전반적으로 비정상적 동작을 하는 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/17

    그룹화 기준: 리소스 ID

    조사 결과 필터:

- 유형이 Unusual Behaviors로 시작
- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

14. 인터넷에서 액세스할 수 있는 포트가 있는 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/18

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 유형이 Software and Configuration Checks/AWS Security Best Practices/Network Reachability로 시작
    - 리소스 유형이 AwsEc2Instance임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

15. 보안 표준/모범 사례를 준수하지 않는 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/19

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 유형이 다음 중 하나로 시작:
      - Software and Configuration Checks/Industry and Regulatory Standards/
      - Software and Configuration Checks/AWSSecurity Best Practices
    - 리소스 유형이 AwsEc2Instance임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

16. 인터넷에 개방된 EC2 인스턴스

    ARN: arn:aws:securityhub:::insight/securityhub/default/21

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 유형이 Software and Configuration Checks/AWS Security Best Practices/Network Reachability로 시작
    - 리소스 유형이 AwsEc2Instance임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

17. 공격자 정찰과 관련된 EC2 인스턴스

ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 TTPs/Discovery/Recon으로 시작
- 리소스 유형이 `AwsEc2Instance`임
- 레코드 상태가 `ACTIVE`임
- 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임

맬웨어와 연결된 18.AWSresources

ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 다음 중 하나로 시작:
  - `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`
- 레코드 상태가 `ACTIVE`임
- 워크플로우 상태가 `NEW` 또는 `NOTIFIED`임

19.암호화 화폐 문제와 관련된 AWS리소스

ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 다음 중 하나로 시작:
  - `Effects/Resource Consumption/Cryptocurrency`

    - TTPs/Command and Control/CryptoCurrency
  - 레코드 상태가 ACTIVE임
  - 워크플로우 상태가 NEW 또는 NOTIFIED임

무단 액세스 시도가 있는 20.AWSresources

ARN: arn:aws:securityhub:::insight/securityhub/default/25

그룹화 기준: 리소스 ID

조사 결과 필터:

- 유형이 다음 중 하나로 시작:
  - TTPs/Command and Control/UnauthorizedAccess
  - TTPs/Initial Access/UnauthorizedAccess
  - Effects/Data Exfiltration/UnauthorizedAccess
  - Unusual Behaviors/User/UnauthorizedAccess
  - Effects/Resource Consumption/UnauthorizedAccess
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

21. 지난 주에 가장 많은 조회수를 기록한 위협 인텔리전스 지표

ARN: arn:aws:securityhub:::insight/securityhub/default/26

조사 결과 필터:

- 지난 7일 이내에 생성됨

22. 조사 결과 개수 기준 상위 계정

ARN: arn:aws:securityhub:::insight/securityhub/default/27

그룹화 기준:AWS 계정 ID

조사 결과 필터:

- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

23. 조사 결과 개수 기준 상위 제품

ARN: arn:aws:securityhub:::insight/securityhub/default/28

그룹화 기준: 제품 이름

조사 결과 필터:

- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

24. 조사 결과 개수 기준 심각도

ARN: arn:aws:securityhub:::insight/securityhub/default/29

그룹화 기준: 심각도 레이블

조사 결과 필터:

- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

25. 조사 결과 개수 기준 상위 S3 버킷

ARN: arn:aws:securityhub:::insight/securityhub/default/30

그룹화 기준: 리소스 ID

조사 결과 필터:

- 리소스 유형이 AwsS3Bucket임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

26. 조사 결과 개수 기준 상위 EC2 인스턴스

ARN: arn:aws:securityhub:::insight/securityhub/default/31

그룹화 기준: 리소스 ID

조사 결과 필터:

- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

27. 조사 결과 개수 기준별 상위 AMI

ARN: arn:aws:securityhub:::insight/securityhub/default/32

그룹화 기준: EC2 인스턴스 이미지 ID

조사 결과 필터:

- 리소스 유형이 AwsEc2Instance임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

28. 조사 결과 개수 기준 상위 IAM 사용자

ARN: arn:aws:securityhub:::insight/securityhub/default/33

그룹화 기준: IAM 액세스 키 ID

조사 결과 필터:

- 리소스 유형이 AwsIamAccessKey임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

29. CIS 점검 실패 횟수 기준 상위 리소스

ARN: arn:aws:securityhub:::insight/securityhub/default/34

그룹화 기준: 리소스 ID

조사 결과 필터:

- 생성기 ID가 arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule로 시작
- 마지막 날에 업데이트됨
- 규정 준수 상태가 FAILED임
- 레코드 상태가 ACTIVE임
- 워크플로우 상태가 NEW 또는 NOTIFIED임

30. 조사 결과 개수 기준 상위 통합

ARN: arn:aws:securityhub:::insight/securityhub/default/35

그룹화 기준: 제품 ARN

조사 결과 필터:

- 레코드 상태가 ACTIVE임

- 워크플로우 상태가 NEW 또는 NOTIFIED임

31. 가장 실패한 보안 검사가 있는 리소스

    ARN: arn:aws:securityhub:::insight/securityhub/default/36

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - 마지막 날에 업데이트됨
    - 규정 준수 상태가 FAILED임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

32. 활동이 의심스러운 IAM 사용자

    ARN: arn:aws:securityhub:::insight/securityhub/default/37

    그룹화 기준: IAM 사용자

    조사 결과 필터:

    - 리소스 유형이 AwsIamUser임
    - 레코드 상태가 ACTIVE임
    - 워크플로우 상태가 NEW 또는 NOTIFIED임

33. 조사 AWS Health결과가 가장 많은 리소스

    ARN: arn:aws:securityhub:::insight/securityhub/default/38

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - ProductName은(는) Health와(과) 같음

34. 조사 AWS Config결과가 가장 많은 리소스

    ARN: arn:aws:securityhub:::insight/securityhub/default/39

    그룹화 기준: 리소스 ID

    조사 결과 필터:

    - ProductName은(는) Config와(과) 같음

35. 가장 많은 조사 결과가 포함된 애플리케이션

    ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

    그룹화 기준: ResourceApplicationArn

    조사 결과 필터:

    - `RecordState`은(는) `ACTIVE`와(과) 같음
    - `Workflow.Status`은(는) `NEW` 또는 `NOTIFIED`와(과) 같음

## Security Hub CSPM의 사용자 지정 인사이트 이해

AWS Security Hub CSPM 관리형 인사이트 외에도 Security Hub CSPM에서 사용자 지정 인사이트를 생성하여 환경에 특정한 문제를 추적할 수 있습니다. 사용자 지정 인사이트는 큐레이션된 하위 집합 추적을 돕습니다.

설정하는 데 유용할 수 있는 사용자 지정 인사이트의 몇 가지 예제는 다음과 같습니다.

- 관리자 계정을 소유하고 있는 경우, 사용자 지정 인사이트를 설정하여 구성원 계정에 영향을 미치는 중요하고 심각도가 높은 조사 결과를 추적할 수 있습니다.
- 특정 통합 AWS 서비스를 사용하는 경우 사용자 지정 인사이트를 설정하여 해당 서비스의 중요하고 심각도가 높은 결과를 추적할 수 있습니다.
- 타사 통합을 사용하는 경우, 사용자 지정 인사이트를 설정하여 해당 통합 제품에서 중요하고 심각도가 높은 조사 결과를 추적할 수 있습니다.

완전히 새로운 사용자 지정 인사이트를 생성하거나 기존 사용자 지정 인사이트 또는 관리형 인사이트를 시작할 수 있습니다.

각 인사이트는 다음 옵션으로 구성됩니다.

- 그룹화 속성 – 그룹화 속성은 인사이트 결과 목록에 표시되는 항목을 결정합니다. 예를 들어, 그룹화 속성이 제품 이름이면 인사이트 조사 결과에 각 조사 결과 공급자와 연관된 조사 결과 수가 표시됩니다.
- 선택적 필터 - 필터는 인사이트과 일치하는 조사 결과의 범위를 좁힙니다.

  조사 결과는 제공된 모든 필터와 일치하는 경우에만 인사이트 조사 결과에 포함됩니다. 예를 들어, 필터가 '제품 이름이 GuardDuty임' 및 '리소스 유형이 `AwsS3Bucket`임'인 경우, 일치하는 조사 결과는 이 두 기준과 일치해야 합니다.

그러나 Security Hub CSPM에서는 속성은 동일하지만 다른 값을 사용하는 필터에 Boolean OR 로직을 적용합니다. 예를 들어, 필터가 '제품 이름이 GuardDuty임'이고 '제품 이름이 Amazon Inspector임'이면 Amazons GuardDuty 또는 Amazon Inspector에 의해 생성된 경우, 조사 결과가 일치합니다.

리소스 식별자 또는 리소스 유형을 그룹화 속성으로 사용하는 경우, 인사이트 조사 결과에는 일치하는 조사 결과에 있는 모든 리소스가 포함됩니다. 이 목록은 리소스 유형 필터와 일치하는 리소스에만 국한되지 않습니다. 예를 들어, 인사이트은 S3 버킷과 관련된 조사 결과를 식별하고 해당 조사 결과를 리소스 식별자별로 그룹화합니다. 일치하는 조사 결과에는 S3 버킷 리소스와 IAM 액세스 키 리소스가 모두 포함됩니다. 인사이트 결과에는 두 리소스가 모두 포함됩니다.

교차 리전 집계를 활성화하고 사용자 지정 인사이트를 생성하면, 집계 리전 및 연결된 리전에서 일치하는 조사 결과에 인사이트가 적용됩니다. 인사이트에 리전 필터가 포함된 경우는 예외입니다.

## 사용자 지정 인사이트 생성

AWS Security Hub CSPM에서 사용자 지정 인사이트를 사용하여 특정 결과 세트를 수집하고 사용자 환경에 고유한 문제를 추적할 수 있습니다. 사용자 지정 인사이트에 대한 배경 정보는 Security Hub CSPM의 사용자 지정 인사이트 이해 섹션을 참조하세요.

원하는 방법을 선택하고 단계에 따라 Security Hub CSPM에서 사용자 지정 인사이트를 생성합니다.

Security Hub CSPM console

사용자 지정 인사이트를 생성하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 인사이트 생성을 선택하세요.
4. 인사이트에 대한 그룹화 속성을 선택하려면
   a. 검색 상자를 선택하여 필터 옵션을 표시합니다.
   b. 그룹화 기준을 선택합니다.
   c. 이 인사이트과 관련되어 있는 조사 결과를 그룹화하는 데 사용할 속성을 선택합니다.
   d. Apply(적용)를 선택합니다.
5. 선택 사항으로, 이 인사이트에 사용할 추가 필터를 선택합니다. 각 필터에 대해 필터 기준을 정의한 다음 적용를 선택합니다.
6. 인사이트 생성을 선택하세요.

7. 인사이트 이름을 입력한 다음 인사이트 생성를 선택하세요.

Security Hub CSPM API

사용자 지정 인사이트를 생성하려면(API)

1. 사용자 지정 인사이트를 생성하려면 Security Hub CSPM API에서 CreateInsight 작업을 사용합니다. 를 사용하는 경우 create-insight 명령을 AWS CLI실행합니다.
2. 사용자 지정 인사이트의 이름을 `Name` 파라미터에 입력합니다.
3. 인사이트에 포함할 조사 결과를 지정하기 위해 `Filters` 파라미터를 채웁니다.
4. `GroupByAttribute` 매개 변수를 채워 인사이트에 포함된 조사 결과를 그룹화하는 데 사용할 속성을 지정합니다.
5. 선택적으로 `SortCriteria` 파라미터를 채워 특정 필드를 기준으로 조사 결과를 정렬할 수 있습니다.

다음 예제에서는 `AwsIamRole` 리소스 유형과 함께 중요한 조사 결과를 포함하는 사용자 지정 인사이트를 생성합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub create-insight --name "Critical role findings" --filters
 '{"ResourceType": [{ "Comparison": "EQUALS", "Value": "AwsIamRole"}],
 "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-
attribute "ResourceId"
```

PowerShell

사용자 지정 인사이트를 생성하려면(PowerShell)

1. `New-SHUBInsight` cmdlet을 사용하세요.
2. 사용자 지정 인사이트의 이름을 `Name` 파라미터에 입력합니다.
3. 인사이트에 포함할 조사 결과를 지정하기 위해 `Filter` 파라미터를 채웁니다.
4. `GroupByAttribute` 매개 변수를 채워 인사이트에 포함된 조사 결과를 그룹화하는 데 사용할 속성을 지정합니다.

교차 리전 집계를 활성화하고 집계 리전에서 이 cmdlet를 사용하는 경우, 집계 및 연결된 리전에서 나온 일치하는 조사 결과에 인사이트이 적용됩니다.

예제

```
$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
```

관리형 인사이트에서 사용자 지정 인사이트 생성(콘솔에서만)

관리형 인사이트에 대한 변경 사항을 저장하거나 관리형 인사이트를 삭제할 수 없습니다. 관리형 인사이트를 사용자 지정 인사이트의 기반으로 사용할 수도 있습니다. 이는 Security Hub CSPM 콘솔에서만 사용할 수 있는 옵션입니다.

관리형 인사이트에서 사용자 지정 인사이트 생성(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 작업할 관리형 인사이트를 선택합니다.
4. 필요에 따라 인사이트 구성을 편집합니다.

   - 인사이트의 조사 결과를 그룹화하는 데 사용한 속성을 변경하려면
     a. 기존의 그룹화를 제거하려면 그룹화 기준 설정 옆에 있는 X를 선택합니다.
     b. 검색 창을 선택합니다.
     c. 그룹화에 사용할 속성을 선택합니다.
     d. 적용을 선택합니다.
   - 인사이트에서 필터를 제거하려면 필터 옆의 원으로 둘러싸인 X를 선택하세요.
   - 인사이트에 필터를 추가하려면
     a. 검색 창을 선택합니다.
     b. 필터로 사용할 속성과 값을 선택합니다.
     c. 적용을 선택합니다.

5. 업데이트가 완료되면 인사이트 생성을 선택합니다.
6. 메시지가 표시되면 인사이트 이름을 입력한 다음 인사이트 생성를 선택합니다.

## 사용자 지정 인사이트 편집

기존 사용자 지정 인사이트를 수정하여 그룹화 값과 필터를 변경할 수 있습니다. 변경한 후 업데이트를 원래 인사이트에 저장하거나 업데이트된 버전을 새로운 인사이트로 저장할 수 있습니다.

AWS Security Hub CSPM에서 사용자 지정 인사이트를 사용하여 특정 결과 세트를 수집하고 사용자 환경에 고유한 문제를 추적할 수 있습니다. 사용자 지정 인사이트에 대한 배경 정보는 Security Hub CSPM의 사용자 지정 인사이트 이해 섹션을 참조하세요.

사용자 지정 인사이트을 편집하려면 원하는 방법을 선택하고 지침을 따르세요.

Security Hub CSPM console

사용자 지정 인사이트를 편집하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 수정할 사용자 지정 인사이트를 선택합니다.
4. 필요에 따라 인사이트 구성을 편집합니다.
   - 인사이트의 조사 결과를 그룹화하는 데 사용한 속성을 변경하려면
     a. 기존의 그룹화를 제거하려면 그룹화 기준 설정 옆에 있는 X를 선택합니다.
     b. 검색 창을 선택합니다.
     c. 그룹화에 사용할 속성을 선택합니다.
     d. 적용을 선택합니다.
   - 인사이트에서 필터를 제거하려면 필터 옆의 원으로 둘러싸인 X를 선택하세요.
   - 인사이트에 필터를 추가하려면
     a. 검색 창을 선택합니다.
     b. 필터로 사용할 속성과 값을 선택합니다.
     c. 적용을 선택합니다.
5. 업데이트를 완료하면 인사이트 저장을 선택합니다.
6. 메시지가 표시되면 다음 중 하나를 수행합니다.

- 기존 인사이트를 업데이트하여 변경 사항을 반영하려면 ***<Insight_Name>*** 업데이트를 선택한 다음 인사이트 저장을 선택합니다.
- 업데이트가 적용된 새로운 인사이트를 생성하려면 새로운 인사이트 저장을 선택합니다. 인사이트 이름을 입력한 다음 인사이트 저장을 선택합니다.

Security Hub CSPM API

사용자 지정 인사이트를 편집하려면(API)

1. Security Hub CSPM API의 `UpdateInsight` 작업을 사용합니다. 를 사용하는 경우 update-insight 명령을 AWS CLI 실행합니다.
2. 업데이트하기 원하는 사용자 지정 인사이트를 식별하려면 인사이트의 Amazon 리소스 이름(ARN)을 입력합니다. 사용자 지정 인사이트의 ARN을 가져오려면 `GetInsights` 작업 또는 get-insights를 사용합니다.
3. 필요에 따라 `Name`, `Filters`, `GroupByAttribute` 파라미터를 업데이트합니다.

다음 예제에서는 지정된 인사이트를 업데이트합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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

사용자 지정 인사이트를 편집하려면(PowerShell)

1. `Update-SHUBInsight` cmdlet을 사용하세요.
2. 사용자 지정 인사이트를 식별할 수 있도록 인사이트의 Amazon 리소스 이름(ARN)을 제공합니다. 사용자 지정 인사이트의 ARN을 가져오려면 `Get-SHUBInsight` cmdlet을 사용하세요.
3. 필요에 따라 `Name`, `Filter`, `GroupByAttribute` 파라미터를 업데이트합니다.

예제

```
$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"
```

## 사용자 지정 인사이트 삭제

AWS Security Hub CSPM에서 사용자 지정 인사이트를 사용하여 특정 결과 세트를 수집하고 사용자 환경에 고유한 문제를 추적할 수 있습니다. 사용자 지정 인사이트에 대한 배경 정보는 Security Hub CSPM의 사용자 지정 인사이트 이해 섹션을 참조하세요.

사용자 지정 인사이트를 삭제하려면 원하는 방법을 선택하고 지침을 따르세요. 관리형 인상이트를 삭제할 수 없습니다.

Security Hub CSPM console

사용자 지정 인사이트를 삭제하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 삭제할 사용자 지정 인사이트를 찾습니다.
4. 이러한 인사이트를 보려면 추가 옵션 아이콘(카드 오른쪽 상단에 있는 점 세 개)을 선택합니다.
5. 삭제를 선택합니다.

Security Hub CSPM API

사용자 지정 인사이트를 삭제하려면(API)

1. Security Hub CSPM API의 `DeleteInsight` 작업을 사용합니다. 를 사용하는 경우 delete-insight 명령을 AWS CLI 실행합니다.
2. 삭제할 사용자 지정 인사이트를 식별하려면 해당 인사이트의 ARN을 제공하세요. 사용자 지정 인사이트의 ARN을 가져오려면 `GetInsights` 작업 또는 get-insights을(를) 사용합니다.

다음 예제에서는 지정한 인사이트를 삭제합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
```

PowerShell

사용자 지정 인사이트를 삭제하려면(PowerShell)

1. `Remove-SHUBInsight` cmdlet을 사용하세요.
2. 사용자 지정 인사이트를 식별하려면 인사이트의 ARN을 제공하세요. 사용자 지정 인사이트의 ARN을 가져오려면 `Get-SHUBInsight` cmdlet을 사용하세요.

예제

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

# Security Hub CSPM 조사 결과 자동 수정 및 조치

AWSSecurity Hub CSPM에는 사양에 따라 조사 결과를 자동으로 수정하고 조치를 취하는 기능이 있습니다.

Security Hub CSPM은 현재 두 유형의 자동화를 지원합니다.

- 자동화 규칙 – 정의한 기준에 따라 거의 실시간으로 조사 결과를 자동으로 업데이트하고 숨깁니다.

- 자동 응답 및 해결 – 특정 조사 결과 및 인사이트에 대해 취해야 할 자동 조치를 정의하는 사용자 지정 Amazon EventBridge 규칙을 생성합니다.

자동화 규칙은 AWSSecurity Finding Format(ASFF)의 결과 필드를 자동으로 업데이트하려는 경우에 유용합니다. 예를 들어, 자동화 규칙을 사용하여 특정 타사 통합의 조사 결과의 심각도 수준 또는 워크플로 상태를 업데이트할 수 있습니다. 자동화 규칙을 사용하면 이 타사 제품의 각 결과의 심각도 수준 또는 워크플로 상태를 수동으로 업데이트할 필요가 없습니다.

EventBridge 규칙은 특정 조사 결과와 관련하여 Security Hub CSPM 외부에서 조치를 취하거나 문제 해결 또는 추가 조사를 위해 서드 파티 도구로 특정 조사 결과를 보내려는 경우에 유용합니다. 이 규칙을 사용하여 AWS Lambda함수 호출 또는 특정 결과에 대한 Amazon Simple Notification Service(Amazon SNS) 주제 알림과 같은 지원되는 작업을 트리거할 수 있습니다.

자동화 규칙은 EventBridge 규칙보다 먼저 적용됩니다. 즉, EventBridge로 전송되기 전에 자동화 규칙이 트리거되고 조사 결과가 업데이트됩니다. 그러면 EventBridge 규칙이 업데이트된 조사 결과에 적용됩니다.

보안 제어 기능을 위한 자동화를 설정할 때는 제목이나 설명보다는 제어 ID를 기준으로 필터링하는 것을 권장합니다. Security Hub CSPM은 때때로 제어 제목 및 설명을 업데이트할 수 있지만 제어 ID는 동일하게 유지됩니다.

주제


- Security Hub CSPM의 자동화 규칙 이해
- 자동 응답 및 문제 해결을 위해 EventBridge 사용


## Security Hub CSPM의 자동화 규칙 이해

자동화 규칙을 사용하여 AWSSecurity Hub CSPM에서 조사 결과를 자동으로 업데이트할 수 있습니다. 조사 결과를 수집하면서 Security Hub CSPM은 조사 결과 숨김, 심각도 변경, 조사 결과에 메모 추가 등 다양한 규칙 작업을 적용할 수 있습니다. 이러한 규칙 작업은 지정된 기준과 일치하는 결과를 수정합니다.

자동화 규칙 사용 사례의 예제는 다음과 같습니다.

- 조사 결과의 리소스 ID가 비즈니스에 중요한 리소스를 참조하는 경우, 조사 결과의 심각도를 `CRITICAL`(으)로 상향 조정합니다.
- 조사 결과가 특정 프로덕션 계정의 리소스에 영향을 미치는 경우, 조사 결과의 심각도를 `HIGH`에서 `CRITICAL`(으)로 상향 조정합니다.

- INFORMATIONAL 심각도를 지닌 특정 조사 결과를 SUPPRESSED 워크플로 상태에 할당합니다.

Security Hub CSPM 관리자 계정에서만 자동화 규칙을 생성하고 관리할 수 있습니다.

규칙은 새로운 조사 결과 및 업데이트된 조사 결과 모두에 적용됩니다. 사용자 지정 규칙을 처음부터 만들거나 Security Hub CSPM에서 제공하는 규칙 템플릿을 사용할 수 있습니다. 템플릿으로 시작하여 필요에 따라 수정할 수도 있습니다.

## 사용 가능한 규칙 기준 및 규칙 작업

Security Hub CSPM 관리자 계정에서 하나 이상의 규칙 기준 및 하나 이상의 규칙 작업을 정의하여 자동화 규칙을 생성할 수 있습니다. 조사 결과가 정의된 기준과 일치하면 Security Hub CSPM은 해당 결과에 규칙 작업을 적용합니다. 사용 가능한 기준 및 작업에 대한 자세한 내용은 사용 가능한 규칙 기준 및 규칙 작업 섹션을 참조하세요.

Security Hub CSPM은 현재 관리자 계정당 최대 100개의 자동화 규칙을 지원합니다.

Security Hub CSPM 관리자 계정은 또한 자동화 규칙을 편집, 보기, 및 삭제할 수 있습니다. 규칙은 관리자 계정과 그에 따른 모든 구성원 계정의 일치하는 조사 결과에 적용됩니다. 멤버 계정 ID를 규칙 기준으로 제공함으로써 Security Hub CSPM 관리자는 또한 자동화 규칙을 사용하여 특정 멤버 계정의 자동화 규칙을 업데이트하거나 조사 결과를 억제할 수 있습니다.

자동화 규칙은이 규칙이 생성된 AWS 리전에만 적용됩니다. 여러 리전에 규칙을 적용하려면 관리자가 각 리전에 규칙을 생성해야 합니다. 이 작업은 Security Hub CSPM 콘솔, Security Hub CSPM API 또는 AWS CloudFormation을 통해 수행할 수 있습니다. 다중 리전 배포 스크립트를 사용할 수도 있습니다.

## 사용 가능한 규칙 기준 및 규칙 작업

자동화 규칙의 기준으로 현재 지원되는 AWSSecurity Finding Format(ASFF) 필드는 다음과 같습니다.

| 규칙 기준 | 필터 연산자 | 필드 유형 |
| --- | --- | --- |
| AwsAccountId | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| AwsAccountName | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, | 문자열 |

| 규칙 기준 | 필터 연산자 | 필드 유형 |
| --- | --- | --- |
| | NOT_EQUALS, PREFIX_NOT_EQUALS | |
| CompanyName | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ComplianceAssociatedStandardsId | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ComplianceSecurityControlId | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ComplianceStatus | Is, Is Not | 선택: [FAILED, NOT_AVAILABLE , PASSED, WARNING] |
| Confidence | Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal) | 숫자 |
| CreatedAt | Start, End, DateRange | 날짜(2022-12-01T21:47:39.269Z 형식) |
| Criticality | Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal) | 숫자 |

| 규칙 기준 | 필터 연산자 | 필드 유형 |
| --- | --- | --- |
| Description | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| FirstObservedAt | Start, End, DateRange | 날짜(2022-12-01T21:47:39.269Z 형식) |
| GeneratorId | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| Id | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| LastObservedAt | Start, End, DateRange | 날짜(2022-12-01T21:47:39.269Z 형식) |
| NoteText | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| NoteUpdatedAt | Start, End, DateRange | 날짜(2022-12-01T21:47:39.269Z 형식) |
| NoteUpdatedBy | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |

| 규칙 기준 | 필터 연산자 | 필드 유형 |
| --- | --- | --- |
| ProductArn | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ProductName | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| RecordState | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| RelatedFindingsId | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| RelatedFindingsProductArn | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ResourceApplicationArn | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ResourceApplicationName | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |

| 규칙 기준 | 필터 연산자 | 필드 유형 |
| --- | --- | --- |
| ResourceDetailsOther | CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS | 맵 |
| ResourceId | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ResourcePartition | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ResourceRegion | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| ResourceTags | CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS | 맵 |
| ResourceType | Is, Is Not | 선택(ASFF에서 지원하는 리소스 참조) |
| SeverityLabel | Is, Is Not | 선택: [CRITICAL, HIGH, MEDIUM, LOW, INFORMATIONAL ] |
| SourceUrl | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |

| 규칙 기준 | 필터 연산자 | 필드 유형 |
| --- | --- | --- |
| Title | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| Type | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| UpdatedAt | Start, End, DateRange | 날짜(2022-12-01T21:47:39.269Z 형식) |
| UserDefinedFields | CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS | 맵 |
| VerificationState | CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS | 문자열 |
| WorkflowStatus | Is, Is Not | 선택: [NEW, NOTIFIED, RESOLVED, SUPPRESSED ] |

문자열 필드로 레이블이 지정된 기준의 경우, 동일한 필드에 다른 필터 연산자를 사용하면 평가 로직에 영향을 미칩니다. 자세한 내용은 AWS Security Hub CSPM API 참조의 StringFilter를 참조하세요.

각 기준은 일치하는 결과를 필터링하는 데 사용할 수 있는 최대 값 수를 지원합니다. 각 기준에 대한 제한은 AWS Security Hub CSPM API 참조의 AutomationRulesFindingFilters를 참조하세요.

현재 자동화 규칙에 대한 작업으로 지원되는 ASFF 필드는 다음과 같습니다.

- Confidence
- Criticality
- Note

- `RelatedFindings`
- `Severity`
- `Types`
- `UserDefinedFields`
- `VerificationState`
- `Workflow`

특정 ASFF 필드에 대한 자세한 내용은 AWS Security Finding Format(ASFF) 구문을 참조하세요.

> **Tip**
>
> Security Hub CSPM에서 특정 제어에 대한 조사 결과 생성을 중지하도록 하려면 자동화 규칙을 사용하는 대신 컨트롤을 사용하지 않도록 설정하는 것이 좋습니다. 제어를 사용하지 않도록 설정하면 Security Hub CSPM은 해당 제어에 대한 보안 검사 실행을 중지하고 조사 결과 생성을 중지하므로 해당 제어에 대한 요금이 발생하지 않습니다. 정의된 기준과 일치하는 조사 결과에 대한 특정 ASFF 필드 값을 변경하려면 자동화 규칙을 사용하는 것이 좋습니다. 컨트롤 비활성화에 대한 자세한 내용은 Security Hub CSPM에서 제어 비활성화 섹션을 참조하세요.

## 자동화 규칙이 평가하는 조사 결과

자동화 규칙은 규칙을 생성한 후 Security Hub CSPM이 BatchImportFindings 작업을 통해 생성하거나 수집하는 새로운 업데이트된 결과를 평가합니다. Security Hub CSPM은 12~24시간마다 또는 관련 리소스의 상태가 변경될 때마다 제어 조사 결과를 업데이트합니다. 자세한 내용은 보안 검사 실행 예약 단원을 참조하십시오.

자동화 규칙은 공급자가 제공한 원본 조사 결과를 평가합니다. 공급자는 Security Hub CSPM API의 `BatchImportFindings` 작업을 사용하여 새로운 조사 결과를 제공하고 기존 조사 결과를 업데이트할 수 있습니다. 원래 조사 결과에 다음 필드가 없는 경우 Security Hub CSPM은 자동화 규칙에 따라 자동으로 필드를 채운 다음 평가에서 채워진 값을 사용합니다.

- `AwsAccountName`
- `CompanyName`
- `ProductName`
- `Resource.Tags`

- `Workflow.Status`

하나 이상의 자동화 규칙을 생성한 후 BatchUpdateFindings 작업을 사용하여 조사 결과 필드를 업데이트하면 규칙이 트리거되지 않습니다. 자동화 규칙을 생성하고 동일한 결과 필드에 영향을 미치는 `BatchUpdateFindings` 업데이트를 수행하는 경우, 마지막 업데이트는 해당 필드의 값을 설정합니다. 다음의 예제를 참조하세요.

1. `BatchUpdateFindings` 작업을 사용하여 조사 결과 `Workflow.Status` 필드의 값을 `NEW`에서 `NOTIFIED`로 변경합니다.
2. `GetFindings`을(를) 직접 호출하는 경우, 이제 `Workflow.Status` 필드의 값은 `NOTIFIED`입니다.
3. 조사 결과의 `Workflow.Status` 필드를 `NEW`에서 `SUPPRESSED`로 변경하는 자동화 규칙을 생성합니다. (규칙은 `BatchUpdateFindings` 작업을 사용하여 적용된 업데이트를 무시합니다.)
4. 조사 결과 공급자는 `BatchImportFindings` 작업을 사용하여 결과를 업데이트하고 조사 결과 `Workflow.Status` 필드의 값을 `NEW`로 변경합니다.
5. `GetFindings`을(를) 직접 호출하는 경우, 이제 `Workflow.Status` 필드의 값은 `SUPPRESSED`입니다. 자동화 규칙이 적용되었고 규칙이 조사 결과에 대해 마지막으로 수행된 작업이기 때문입니다.

Security Hub CSPM 콘솔에서 규칙을 생성하거나 편집하면 콘솔에 규칙 기준과 일치하는 베타 조사 결과가 표시됩니다. 자동화 규칙은 결과 공급자가 보낸 원래 결과를 평가하는 반면 콘솔 베타는 GetFindings 작업에 대한 응답에 표시되는 최종 상태의 결과를 반영합니다(즉, 규칙 작업 또는 기타 업데이트가 결과에 적용된 후).

## 규칙 순서 작동 방식

자동화 규칙을 생성할 때 각 규칙에 순서를 할당합니다. 이는 Security Hub CSPM이 자동화 규칙을 적용하는 순서를 결정하며, 여러 규칙이 동일한 결과 또는 결과 필드와 관련된 경우, 중요해집니다.

여러 규칙 작업이 동일한 결과 또는 결과 필드와 관련된 경우, 규칙 순서의 숫자 값이 가장 높은 규칙이 마지막에 적용되어 궁극적인 효과를 발휘합니다.

Security Hub CSPM 콘솔에서 규칙을 생성하면 Security Hub CSPM은 규칙 생성 순서에 따라 규칙 순서를 자동으로 할당합니다. 가장 최근에 만든 규칙이 규칙 순서 숫자 값이 가장 낮으므로 먼저 적용됩니다. Security Hub CSPM은 후속 규칙을 오름차순으로 적용합니다.

Security Hub CSPM API 또는를 통해 규칙을 생성하면 AWS CLISecurity Hub CSPM은 `RuleOrder` 먼저 가장 낮은 숫자 값으로 규칙을 적용합니다. 그런 다음 다음 규칙을 오름차순으로 적용합니다. 여

러 조사 결과에 동일한 RuleOrder가 있는 경우, Security Hub CSPM은 UpdatedAt 필드에 이전 값이 있는 규칙을 먼저 적용합니다(즉, 가장 최근에 편집된 규칙이 마지막에 적용됨).

언제든지 규칙 순서를 변경할 수 있습니다.

규칙 순서의 예제:

규칙 A(규칙 순서는 **1**):

- 규칙 A 기준
  - ProductName = Security Hub CSPM
  - Resources.Type은(는) S3 Bucket
  - Compliance.Status = FAILED
  - RecordState은(는) NEW
  - Workflow.Status = ACTIVE
- 규칙 A 작업
  - Confidence을(를) 95(으)로 업데이트
  - Severity을(를) CRITICAL(으)로 업데이트

규칙 B(규칙 순서는 **2**):

- 규칙 B 기준
  - AwsAccountId = 123456789012
- 규칙 B 작업
  - Severity을(를) INFORMATIONAL(으)로 업데이트

규칙 A 작업은 규칙 A 기준과 일치하는 Security Hub CSPM 조사 결과에 먼저 적용됩니다. 다음으로, 규칙 B 작업은 지정된 계정 ID를 가진 Security Hub CSPM 조사 결과에 적용됩니다. 이 예제에서는 규칙 B가 마지막에 적용되므로 지정된 계정 ID의 조사 결과에서 Severity의 최종 값은 INFORMATIONAL입니다. 규칙 A 작업에 따라 일치하는 조사 결과에서 Confidence의 최종 값은 95입니다.

## 자동화 규칙 생성

자동화 규칙을 사용하여 AWSSecurity Hub CSPM에서 조사 결과를 자동으로 업데이트할 수 있습니다. 사용자 지정 규칙을 처음부터 새로 만들거나 Security Hub CSPM 콘솔에서 미리 채워진 규칙 템플릿을

사용할 수 있습니다. 자동화 규칙의 작동 방식에 대한 배경 정보는 Security Hub CSPM의 자동화 규칙 이해 섹션을 참조하세요.

한 번에 하나의 자동화 규칙만 생성할 수 있습니다. 자동화 규칙을 여러 개 만들려면 콘솔 절차를 여러 번 따르거나 원하는 파라미터를 사용하여 API 또는 명령을 여러 번 직접 호출하세요.

조사 결과에 규칙을 적용하려는 각 리전 및 계정에서 자동화 규칙을 생성해야 합니다.

Security Hub CSPM 콘솔에서 자동화 규칙을 만들면 Security Hub CSPM은 규칙이 적용되는 베타 조사 결과를 표시합니다. 규칙 기준에 CONTAINS 또는 NOT_CONTAINS 필터가 포함된 경우, 베타는 현재 지원되지 않습니다. 맵 및 문자열 필드 유형에 대해 이러한 필터를 선택할 수 있습니다.

> **Important**
>
> AWS에서는 규칙 이름, 설명 또는 기타 필드에 개인 식별 정보, 기밀 정보 또는 민감한 정보를 포함하지 않을 것을 권장합니다.

### 사용자 지정 자동화 규칙 생성

원하는 방법을 선택하고 다음 단계를 완료하여 사용자 지정 자동화 규칙을 생성합니다.

Console

사용자 지정 자동화 규칙을 생성하려면(콘솔)

1. Security Hub CSPM 관리자의 자격 증명을 사용하여 https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 규칙 생성을 선택합니다. 규칙 유형에서 사용자 지정 규칙 생성을 선택합니다.
4. 규칙 섹션에서 규칙에 대한 고유한 규칙 이름과 설명을 입력합니다.
5. 기준에서 키, 연산자 및 값 드롭다운 메뉴를 사용하여 규칙 기준을 지정합니다. 규칙 기준을 하나 이상 지정해야 합니다.

   선택한 기준에 대해 지원되는 경우, 콘솔에 기준과 일치하는 베타 조사 결과가 표시됩니다.
6. 자동 작업의 경우, 드롭다운 메뉴를 사용하여 조사 결과가 규칙 기준과 일치할 때 업데이트할 조사 결과 필드를 지정합니다. 규칙 작업을 최소 하나 이상 지정해야 합니다.
7. 규칙 상태에서는 규칙을 생성한 후 해당 규칙을 활성화할지 또는 비활성화할지 선택합니다.

8. (선택 사항)추가 설정 섹션을 확장합니다. 이 규칙을 규칙 기준과 일치하는 조사 결과에 마지막으로 적용하려면 이러한 기준과 일치하는 조사 결과에 대한 후속 규칙 무시를 선택합니다.
9. (선택 사항)규칙을 쉽게 식별할 수 있도록 태그의 경우, 태그를 키-값 쌍으로 추가합니다.
10. 규칙 생성을 선택합니다.

API

사용자 지정 자동화 규칙을 생성하려면(API)

1. Security Hub CSPM 관리자 계정에서 `CreateAutomationRule`을 실행합니다. 이 API는 특정 Amazon 리소스 이름(ARN)을 사용하여 규칙을 생성합니다.
2. 규칙의 이름 및 설명을 입력합니다.
3. 이 규칙이 규칙 기준과 일치하는 조사 결과에 적용되는 마지막 규칙이 되도록 하려면 `IsTerminal` 파라미터를 `true`(으)로 설정하세요.
4. `RuleOrder` 파라미터에 대해 규칙의 순서를 입력합니다. Security Hub CSPM은 이 파라미터에 더 낮은 번호의 규칙을 먼저 적용합니다.
5. `RuleStatus` 파라미터에서 Security Hub CSPM이 조사 결과 생성 후 규칙을 활성화하고 적용을 시작할지 여부를 지정합니다. 값을 지정하지 않을 경우, 기본값은 `ENABLED`입니다. `DISABLED` 값은 규칙이 생성된 후 일시 중지되는 것을 의미합니다.
6. `Criteria` 파라미터에 Security Hub CSPM이 조사 결과를 필터링하는 데 사용할 기준을 입력합니다. 규칙 작업은 기준과 일치하는 조사 결과에 적용됩니다. 지원되는 기준 목록은 사용 가능한 규칙 기준 및 규칙 작업 섹션을 참조하세요.
7. `Actions` 파라미터에는 조사 결과와 정의된 기준 간에 일치하는 항목이 있을 때 Security Hub CSPM이 수행할 작업을 입력합니다. 지원되는 작업 목록은 사용 가능한 규칙 기준 및 규칙 작업을 참조하세요.

다음 예제 AWS CLI명령은 자동화 규칙을 생성하여 워크플로 상태를 업데이트하고 일치하는 조사 결과를 기록합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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
```

템플릿에서 규칙 생성(콘솔만 해당)

규칙 템플릿은 자동화 규칙에 대한 일반적인 사용 사례를 반영합니다. 현재는 Security Hub CSPM 콘솔에서만 규칙 템플릿을 지원합니다. 다음 단계를 완료하여 콘솔의 템플릿에서 자동화 규칙을 생성합니다.

템플릿에서 자동화 규칙을 생성하려면(콘솔)

1. Security Hub CSPM 관리자의 자격 증명을 사용하여 https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 규칙 생성을 선택합니다. 규칙 유형에서 템플릿에서 규칙 생성을 선택합니다.
4. 드롭다운 메뉴에서 규칙 템플릿을 선택합니다.
5. (선택 사항)사용 사례에 필요한 경우, 규칙, 기준 및 자동 작업 섹션을 수정하세요. 규칙 기준과 규칙 작업을 하나 이상 지정해야 합니다.

   선택한 기준에 대해 지원되는 경우, 콘솔에 기준과 일치하는 베타 조사 결과가 표시됩니다.
6. 규칙 상태에서는 규칙을 생성한 후 해당 규칙을 활성화할지 또는 비활성화할지 선택합니다.

7. (선택 사항)추가 설정 섹션을 확장합니다. 이 규칙을 규칙 기준과 일치하는 조사 결과에 마지막으로 적용하려면 이러한 기준과 일치하는 조사 결과에 대한 후속 규칙 무시를 선택합니다.
8. (선택 사항)규칙을 쉽게 식별할 수 있도록 태그의 경우, 태그를 키-값 쌍으로 추가합니다.
9. 규칙 생성을 선택합니다.

## 자동화 규칙 보기

자동화 규칙을 사용하여 AWSSecurity Hub CSPM에서 조사 결과를 자동으로 업데이트할 수 있습니다. 자동화 규칙의 작동 방식에 대한 배경 정보는 Security Hub CSPM의 자동화 규칙 이해 섹션을 참조하세요.

원하는 방법을 선택하고 단계에 따라 자동화 규칙과 각 규칙의 세부 정보를 확인하세요.

자동화 규칙으로 인해 조사 결과가 어떻게 변경되었는지에 대한 기록을 보려면 Security Hub CSPM에서 조사 결과 세부 정보 및 기록 검토 섹션을 참조하세요.

Console

자동화 규칙을 보려면(콘솔)

1. Security Hub CSPM 관리자의 자격 증명을 사용하여 https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 규칙 이름을 선택합니다. 아니면 규칙을 선택할 수도 있습니다.
4. 작업 및 보기를 선택합니다.

API

자동화 규칙을 보려면(API)

1. 계정의 자동화 규칙을 보려면 Security Hub CSPM 관리자 계정에서 `ListAutomationRules`를 실행합니다. 이 API는 규칙에 대한 규칙 ARN 및 기타 메타데이터를 반환합니다. 이 API에는 입력 파라미터가 필요하지 않지만, 선택적으로 결과 수를 제한하기 위해 `MaxResults`을(를) 제공하고 `NextToken`을(를) 페이지 매김 파라미터로 제공할 수 있습니다. `NextToken`의 초기값은 `NULL`이어야 합니다.

2. 규칙의 기준 및 작업을 비롯한 추가 규칙 세부 정보를 보려면 Security Hub CSPM 관리자 계정에서 BatchGetAutomationRules를 실행합니다. 세부 정보를 원하는 자동화 규칙의 ARN을 제공합니다.

   다음 예제에서는 지정된 자동화 규칙에 대한 세부 정보를 검색합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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
```

## 자동화 규칙 편집

자동화 규칙을 사용하여 AWSSecurity Hub CSPM에서 조사 결과를 자동으로 업데이트할 수 있습니다. 자동화 규칙의 작동 방식에 대한 배경 정보는 Security Hub CSPM의 자동화 규칙 이해 섹션을 참조하세요.

자동화 규칙을 생성한 후 위임된 Security Hub CSPM 관리자는 규칙을 편집할 수 있습니다. 자동화 규칙을 편집하면 규칙 편집 후 Security Hub CSPM가 생성하거나 수집한 새로운 및 업데이트된 조사 결과에 변경 사항이 적용됩니다.

원하는 방법을 선택하고 단계에 따라 자동화 규칙의 내용을 편집하세요. 요청 한 번으로 하나 이상의 규칙을 편집할 수 있습니다. 규칙 순서 편집에 대한 지침은 자동화 규칙 순서 편집 섹션을 참조하세요.

Console

자동화 규칙을 편집하려면(콘솔)

1. Security Hub CSPM 관리자의 자격 증명을 사용하여 https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 편집할 규칙을 선택합니다. 작업을 선택한 후 편집을 선택합니다.
4. 원하는 대로 규칙을 변경하고 변경 내용 저장을 선택합니다.

API

자동화 규칙 편집(API)

1. Security Hub CSPM 관리자 계정에서 BatchUpdateAutomationRules을 실행합니다.
2. RuleArn 파라미터에는 편집하려는 규칙의 ARN을 입력합니다.
3. 편집하려는 파라미터의 새로운 값을 입력합니다. RuleArn을(를) 제외한 모든 파라미터를 편집할 수 있습니다.

다음 예제에서는 지정된 자동화 규칙을 업데이트합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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
```

# 자동화 규칙 순서 편집

자동화 규칙을 사용하여 AWSSecurity Hub CSPM에서 조사 결과를 자동으로 업데이트할 수 있습니다. 자동화 규칙의 작동 방식에 대한 배경 정보는 Security Hub CSPM의 자동화 규칙 이해 섹션을 참조하세요.

자동화 규칙을 생성한 후 위임된 Security Hub CSPM 관리자는 규칙을 편집할 수 있습니다.

경우에 따라 규칙 기준과 작업은 그대로 유지하되 Security Hub CSPM에서 자동화 규칙을 적용하는 순서를 변경하길 원할 경우, 자동화 규칙만을 편집할 수 있습니다. 원하는 방법을 선택하고 단계에 따라 규칙 순서를 편집합니다.

자동화 규칙의 기준 또는 작업 편집에 대한 지침은 자동화 규칙 편집 섹션을 참조하세요.

Console

자동화 규칙 순서를 편집하려면(콘솔)

1. Security Hub CSPM 관리자의 자격 증명을 사용하여 https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 순서를 변경할 규칙을 선택합니다. 우선 순위 편집을 선택합니다.
4. 위로 이동을 선택하여 규칙의 우선 순위를 한 단위 높입니다. 아래로 이동을 선택하여 규칙 우선 순위를 한 단위 낮춥니다. 맨 위로 이동을 선택하여 규칙에 순서를 1로 지정합니다(이렇게 하면 해당 규칙이 다른 기존 규칙보다 우선함)

> **Note**
>
> Security Hub CSPM 콘솔에서 규칙을 생성하면 Security Hub CSPM은 규칙 생성 순서에 따라 규칙 순서를 자동으로 할당합니다. 가장 최근에 만든 규칙이 규칙 순서 숫자 값이 가장 낮으므로 먼저 적용됩니다.

API

자동화 규칙 순서를 편집하려면(API)

1. Security Hub CSPM 관리자 계정에서 `BatchUpdateAutomationRules` 작업을 사용합니다.
2. `RuleArn` 파라미터에는 순서를 편집하려는 규칙의 ARN을 입력합니다.

3. `RuleOrder` 필드 값을 수정합니다.

> **Note**
>
> 여러 규칙에 동일한 `RuleOrder`가 있는 경우, Security Hub CSPM은 `UpdatedAt` 필드에 이전 값이 있는 규칙을 먼저 적용합니다(즉, 가장 최근에 편집된 규칙이 마지막에 적용됨).

## 자동화 규칙 삭제 또는 비활성화

자동화 규칙을 사용하여 AWSSecurity Hub CSPM에서 조사 결과를 자동으로 업데이트할 수 있습니다. 자동화 규칙의 작동 방식에 대한 배경 정보는 Security Hub CSPM의 자동화 규칙 이해 섹션을 참조하세요.

자동화 규칙을 삭제하면 Security Hub CSPM은 계정에서 해당 규칙을 삭제하고 조사 결과에 더 이상 규칙을 적용하지 않습니다. 규칙을 삭제하는 대신 규칙을 비활성화할 수 있습니다. 이렇게 하면 나중에 사용할 수 있도록 규칙이 유지되지만, Security Hub CSPM은 사용자가 활성화하기 전까지는 일치하는 조사 결과에 규칙을 적용하지 않습니다.

원하는 방법을 선택하고 단계에 따라 자동화 규칙을 삭제합니다. 단일 요청으로 하나 이상의 규칙을 삭제할 수 있습니다.

Console

자동화 규칙을 삭제하거나 비활성화하려면(콘솔)

1. Security Hub CSPM 관리자의 자격 증명을 사용하여 https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 자동화를 선택합니다.
3. 삭제할 규칙을 선택합니다. 작업 및 삭제를 선택합니다(규칙을 유지하지만 일시적으로 비활성화하려면 비활성화 선택).
4. 선택을 확인하고 삭제를 선택합니다.

API

자동화 규칙을 삭제하거나 비활성화하려면(API)

1. Security Hub CSPM 관리자 계정에서 `BatchDeleteAutomationRules` 작업을 사용합니다.

2. `AutomationRulesArns` 파라미터에 삭제하려는 규칙의 ARN을 입력합니다(규칙을 유지하지만 일시적으로 비활성화하려면 `RuleStatus` 파라미터에 대한 `DISABLED`을(를) 입력).

다음 예제에서는 지정된 자동화 규칙을 삭제합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ 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
```

## 자동화 규칙 예제

이 섹션에서는 일반적인 Security Hub CSPM 사용 사례에 대한 자동화 규칙의 예제를 제공합니다. 이러한 예제는 Security Hub CSPM 콘솔에서 사용할 수 있는 규칙 템플릿에 해당합니다.

S3 버킷과 같은 특정 리소스가 위험에 처한 경우, 심각도를 Critical로 상향 조정합니다.

이 예제에서는 결과의 `ResourceId`이(가) 특정 Amazon Simple Storage Service(S3) 버킷일 때 규칙 기준을 일치시킵니다. 규칙 작업은 일치하는 조사 결과의 심각도를 `CRITICAL`(으)로 변경하는 것입니다. 이 템플릿을 수정하여 다른 리소스에 적용할 수 있습니다.

API 요청 예제:

```
{
    "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"
            }
        }
    }]
}
```

CLI 명령 예제:

```
$
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
```

프로덕션 계정의 리소스와 관련된 조사 결과의 심각도를 상향 조정합니다.

이 예제에서는 특정 프로덕션 계정에서 HIGH 심각도 조사 결과가 생성될 때 규칙 기준을 일치시킵니다. 규칙 작업은 일치하는 조사 결과의 심각도를 CRITICAL(으)로 변경하는 것입니다.

API 요청 예제:

```
{
    "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"
           }
```

```
        }
    }]
}
```

CLI 명령 예제:

```
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
```

정보 조사 결과 표시 안 함

이 예제에서는 Amazon GuardDuty에서 Security Hub CSPM으로 전송한 INFORMATIONAL 심각도 조사 결과와 규칙 기준을 일치시킵니다. 규칙 작업은 일치하는 조사 결과의 워크플로 상태를 SUPPRESSED(으)로 변경하는 것입니다.

API 요청 예제:

```
{
    "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"
            }
        }
    }]
}
```

CLI 명령 예제:

```
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
```

## 자동 응답 및 문제 해결을 위해 EventBridge 사용

Amazon EventBridge에서 규칙을 생성하면 AWS Security Hub CSPM 결과에 자동으로 응답할 수 있습니다. Security Hub CSPM은 거의 실시간으로 조사 결과를 EventBridge에 이벤트로 전송합니다. 원하는 이벤트만 표시하도록 간단한 규칙을 작성한 후 규칙과 일치하는 이벤트 발생 시 실행할 자동화 작업을 지정할 수 있습니다. 자동으로 트리거할 수 있는 태스크는 다음과 같습니다.

- AWS Lambda 함수 호출
- Amazon EC2 실행 명령 간접 호출
- Amazon Kinesis Data Streams로 이벤트 릴레이
- AWS Step Functions 상태 시스템 활성화
- SNS 주제 또는 Amazon SQS 대기열 알림
- 타사 티켓팅, 채팅, SIEM 또는 인시던트 대응 및 관리 도구에 조사 결과 전송

Security Hub CSPM은 모든 새로운 조사 결과와 기존 조사 결과의 모든 업데이트를 EventBridge에 EventBridge 이벤트로 자동 전송합니다. 선택한 조사 결과와 인사이트 조사 결과를 EventBridge로 전송할 수 있게 하는 사용자 지정 작업을 생성할 수도 있습니다.

그러면 각 유형의 이벤트에 대응하도록 EventBridge 규칙을 구성합니다.

EventBridge 사용에 대한 자세한 내용은 Amazon EventBridge User Guide를 참조하세요.

> **Note**
>
> 가장 좋은 방법은 EventBridge에 액세스할 수 있도록 사용자에게 부여된 권한이 필요한 권한만 부여하는 최소 권한 AWS Identity and Access Management (IAM) 정책을 사용하는지 확인하는 것입니다.
> 자세한 내용은 Amazon EventBridge의 Identity and Access Management를 참조하세요.

교차 계정 자동 응답 및 문제 해결을 위한 템플릿 세트는 AWS 솔루션에서도 사용할 수 있습니다. 템플릿은 EventBridge 이벤트 규칙 및 Lambda 함수를 활용합니다. CloudFormation 및를 사용하여 솔루션을 배포합니다 AWS Systems Manager. 이 솔루션은 완전 자동 응답 및 해결 조치를 생성할 수 있습니다. 또한 Security Hub CSPM 사용자 지정 작업을 사용하여 사용자가 트리거하는 응답 및 해결 조치를 생성할 수 있습니다. 솔루션을 구성하고 사용하는 방법에 대한 자세한 내용은 AWS솔루션 페이지의 자동 보안 대응을 참조하세요.

주제

- EventBridge의 Security Hub CSPM 이벤트 유형
- Security Hub CSPM용 EventBridge 이벤트 형식
- Security Hub CSPM 조사 결과에 대한 EventBridge 규칙 구성
- 사용자 지정 작업을 사용하여 조사 결과 및 인사이트 조사 결과를 EventBridge로 전송

## EventBridge의 Security Hub CSPM 이벤트 유형

Security Hub CSPM은 다음과 같은 Amazon EventBridge 이벤트 유형을 사용하여 EventBridge와 통합합니다.

Security Hub CSPM의 EventBridge 대시보드에서 모든 이벤트에는 이러한 이벤트 유형이 모두 포함됩니다.

모든 조사 결과(Security Hub Findings - Imported)

Security Hub CSPM은 모든 새로운 조사 결과와 기존 조사 결과의 모든 업데이트를 EventBridge에 Security Hub Findings - Imported 이벤트로 자동 전송합니다. 각 Security Hub Findings - Imported 이벤트에는 단일 조사 결과가 포함됩니다.

모든 `BatchImportFindings` 및 `BatchUpdateFindings` 요청은 Security Hub Findings - Imported 이벤트를 트리거합니다.

관리자 계정의 경우, EventBridge의 이벤트 피드에는 관리자 계정과 회원 계정 모두에서 찾은 조사 결과에 대한 이벤트가 포함됩니다.

집계 지역의 이벤트 피드에는 집계 지역 및 연결 지역의 조사 결과에 대한 이벤트가 포함됩니다. 지역 간 조사 결과는 거의 실시간으로 이벤트 피드에 포함됩니다. 조사 결과 집계를 구성하는 방법에 대한 자세한 내용은 the section called “리전 간 데이터 집계” 섹션을 참조하세요.

조사 결과를 문제 해결 워크플로, 타사 도구, 또는 기타 지원되는 EventBridge 대상으로 자동 라우팅하는 규칙을 정의할 수 있습니다. 조사 결과에 특정 속성 값이 있는 경우에만 규칙을 적용하는 필터가 규칙에 포함될 수 있습니다.

이 방법을 사용하여 모든 조사 결과 또는 특정한 특성이 있는 모든 조사 결과를 자동으로 응답 또는 문제 해결 워크플로우로 보냅니다.

the section called “EventBridge 규칙 구성” 섹션을 참조하세요.

사용자 지정 작업에 대한 조사 결과(Security Hub Findings - Custom Action)

또한 Security Hub CSPM은 사용자 지정 작업과 연결된 조사 결과를 EventBridge에 Security Hub Findings - Custom Action 이벤트로 전송합니다.

이는 Security Hub CSPM 콘솔을 사용해 특정 조사 결과나 작은 조사 결과 세트를 응답 또는 문제 해결 워크플로로 보내려는 분석가에게 유용합니다. 한 번에 최대 20개의 조사 결과에 대해 사용자 지정 작업을 선택할 수 있습니다. 각 조사 결과는 별도의 EventBridge 이벤트로 EventBridge에 전송됩니다.

사용자 지정 작업을 생성할 때 사용자 지정 작업 ID를 할당합니다. 이 ID를 사용하여 사용자 지정 작업 ID와 관련된 조사 결과를 수신한 후 지정된 작업을 수행하는 EventBridge 규칙을 생성할 수 있습니다.

the section called “사용자 지정 작업 구성 및 사용”을(를) 참조하세요.

예를 들어, Security Hub CSPM에서 `send_to_ticketing`이라는 사용자 지정 작업을 생성할 수 있습니다. 그런 다음, EventBridge에서 `send_to_ticketing` 사용자 지정 작업 ID가 포함된 조사 결과를 EventBridge가 수신할 때 트리거되는 규칙을 생성합니다. 이 규칙에는 조사 결과를 티켓팅 시스템에 전송하는 로직이 포함됩니다. 그런 다음 Security Hub CSPM 내에서 조사 결과를 선택하고 Security Hub CSPM의 사용자 지정 작업을 사용하여 조사 결과를 티켓팅 시스템에 수동으로 전송할 수 있습니다.

추가 처리를 위해 Security Hub CSPM 조사 결과를 EventBridge로 보내는 방법의 예는 AWS Security Hub CSPM 사용자 지정 작업을 PagerDuty와 통합하는 방법 및 AWS 파트너 네트워크(APN) 블로그의 AWS Security Hub CSPM에서 사용자 지정 작업을 활성화하는 방법을 참조하세요.

사용자 지정 작업에 대한 인사이트 결과(Security Hub Insight Results)

또한 사용자 지정 작업을 사용하여 인사이트 결과 집합을 EventBridge에 Security Hub Insight Results 이벤트로 전송할 수 있습니다. 인사이트 결과는 인사이트와 일치하는 리소스입니다. 인사이트 조사 결과를 EventBridge에 전송할 때는 조사 결과를 EventBridge에 전송하는 것이 아닙니다. 인사이트 결과와 연결된 리소스 식별자만 전송합니다. 한 번에 최대 100개의 리소스 식별자를 전송할 수 있습니다.

조사 결과에 대한 사용자 지정 작업과 마찬가지로, 먼저 Security Hub CSPM에서 사용자 지정 작업을 생성한 다음, EventBridge에서 규칙을 생성합니다.

the section called “사용자 지정 작업 구성 및 사용”을(를) 참조하세요.

예를 들어, 동료와 공유하고 싶은 관심 대상 특정 인사이트 결과를 보았다고 가정해 보겠습니다. 이 경우, 사용자 지정 작업을 사용하여 채팅 또는 티켓 시스템을 통해 해당 인사이트 결과를 동료에게 보낼 수 있습니다.

## Security Hub CSPM용 EventBridge 이벤트 형식

Security Hub Findings - Imported, Security Findings - Custom Action 및 Security Hub Insight Results 이벤트 유형은 다음 이벤트 형식을 사용합니다.

이벤트 형식은 Security Hub CSPM이 EventBridge로 이벤트를 전송할 때 사용되는 형식입니다.

Security Hub Findings - Imported

Security Hub CSPM에서 EventBridge로 전송되는 Security Hub Findings - Imported 이벤트는 다음 형식을 사용합니다.

```
{
   "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>*는 이벤트에서 전송한 조사 결과의 내용(JSON 형식)입니다. 각 이벤트는 단일 조사 결과를 전송합니다.

조사 결과의 전체 목록은 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

이러한 이벤트에 의해 트리거되는 EventBridge 규칙 구성 방법에 대한 자세한 내용은 the section called “EventBridge 규칙 구성” 섹션을 참조하세요.

Security Hub Findings - Custom Action

Security Hub CSPM에서 EventBridge로 전송되는 Security Hub Findings - Custom Action 이벤트는 다음 형식을 사용합니다. 각 조사 결과는 별도의 이벤트로 전송됩니다.

```
{
  "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>*는 이벤트에서 전송한 조사 결과의 내용(JSON 형식)입니다. 각 이벤트는 단일 조사 결과를 전송합니다.

조사 결과의 전체 목록은 AWS 보안 조사 결과 형식(ASFF) 섹션을 참조하세요.

이러한 이벤트에 의해 트리거되는 EventBridge 규칙 구성 방법에 대한 자세한 내용은 the section called “사용자 지정 작업 구성 및 사용” 섹션을 참조하세요.

Security Hub Insight Results

Security Hub CSPM에서 EventBridge로 전송되는 Security Hub Insight Results 이벤트는 다음 형식을 사용합니다.

```
{
  "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}
    ]
  }
}
```

이러한 이벤트에 의해 트리거되는 EventBridge 규칙 생성에 대한 자세한 내용은 the section called “사용자 지정 작업 구성 및 사용” 섹션을 참조하세요.

## Security Hub CSPM 조사 결과에 대한 EventBridge 규칙 구성

Amazon EventBridge에서 Security Hub Findings - Imported 이벤트를 수신할 때 수행할 작업을 정의하는 규칙을 생성할 수 있습니다. Security Hub Findings - Imported 이벤트는 `BatchImportFindings` 및 `BatchUpdateFindings` 작업으로부터의 업데이트에 의해 트리거됩니다.

각 규칙에는 규칙을 트리거하는 이벤트를 식별하는 이벤트 패턴이 포함되어 있습니다. 이벤트 패턴에는 항상 이벤트 소스(`aws.securityhub`)와 이벤트 유형(Security Hub 조사 결과 - 가져옴)이 포함됩니다. 이벤트 패턴은 규칙이 적용되는 조사 결과를 식별하는 필터를 지정할 수도 있습니다.

그러면 이벤트 규칙이 규칙 대상을 식별합니다. 대상은 EventBridge가 Security Hub 조사 결과 - 가져옴 이벤트를 수신하고 조사 결과가 필터와 일치할 때 취할 조치입니다.

여기에 제공된 지침은 EventBridge 콘솔을 사용합니다. 콘솔을 사용하면 EventBridge는 EventBridge가 Amazon CloudWatch Logs에 기록을 활성화할 수 있도록 필요한 리소스 기반 정책을 자동으로 생성합니다.

또한 EventBridge API의 `PutRule` 작업을 사용할 수도 있습니다. 하지만 EventBridge API를 사용하는 경우, 리소스 기반 정책을 생성해야 합니다. 필수 정책에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 CloudWatch Logs 권한을 참조하세요.

이벤트 패턴 형식

Security Hub 조사 결과 - 가져옴 이벤트의 이벤트 패턴 형식은 다음과 같습니다.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source`는 Security Hub CSPM을 이벤트를 생성하는 서비스로 식별합니다.
- `detail-type`은(는) 이벤트 유형을 식별합니다.

- `detail`은(는) 선택 사항이며 이벤트 패턴에 대한 필터 값을 제공합니다. 이벤트 패턴에 `detail` 필드가 없는 경우, 모든 조사 결과가 규칙을 트리거합니다.

모든 조사 결과 속성을 기준으로 조사 결과를 필터링할 수 있습니다. 각 값에 대해 하나 이상의 값을 쉼표로 구분한 배열을 제공합니다.

```
"<attribute name>": [ "<value1>", "<value2>"]
```

속성에 둘 이상의 값을 제공하면 해당 값이 OR로 결합됩니다. 조사 결과에 나열된 값 중 하나라도 있는 경우, 조사 결과는 개별 속성의 필터와 일치합니다. 예를 들어, `INFORMATIONAL`과 `LOW`를 모두 `Severity.Label` 값으로 제공하면 심각도 레이블이 `INFORMATIONAL` 또는 `LOW`일 경우, 조사 결과가 일치합니다.

속성은 AND로 결합됩니다. 제공된 모든 속성에 대한 필터 기준과 일치하면 조사 결과가 일치합니다.

속성 값을 제공할 때는 AWS Security Finding Format(ASFF) 구조 내에서 해당 속성의 위치를 반영해야 합니다.

> **Tip**
>
> 제어 조사 결과를 필터링할 때는 `Title` 또는 `Description` 대신 `SecurityControlId` 또는 `SecurityControlArn` ASFF 필드를 필터로 사용하는 것이 좋습니다. 후자의 필드는 때때로 변경될 수 있지만 제어 ID 및 ARN은 정적 식별자입니다.

다음 예제에서 이벤트 패턴은 `ProductArn` 및 `Severity.Label`에 대한 필터 값을 제공하므로 Amazon Inspector에서 생성되고 심각도 레이블이 `INFORMATIONAL` 또는 `LOW`인 경우, 조사 결과가 일치합니다.

```
{
    "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"]
            }
        }
    }
}
```

이벤트 규칙 생성

사전 정의된 이벤트 패턴 또는 사용자 지정 이벤트 패턴을 사용하여 EventBridge에서 규칙을 생성할 수 있습니다. 사전 정의된 패턴을 선택하면 EventBridge가 자동으로 `source` 및 `detail-type`을 채웁니다. EventBridge는 다음과 같은 조사 결과 속성에 대한 필터 값을 지정하는 필드도 제공합니다.

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

EventBridge 규칙 생성(콘솔)

1. Amazon EventBridge 콘솔(https://console.aws.amazon.com/events/)을 엽니다.
2. 다음 값을 사용하여 조사 결과 이벤트를 모니터링하는 EventBridge 규칙을 생성합니다.
   - 규칙 유형에서 이벤트 패턴이 있는 규칙을 생성합니다.
   - 이벤트 패턴 작성 방법을 선택합니다.

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
|---|---|---|
| 템플릿 | 이벤트 패턴 섹션에서 다음을 선택합니다. | |

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
| --- | --- | --- |
| | • 이벤트 소스에서 AWS 서비스를 선택합니다.<br>• AWS 서비스에 대해 Security Hub를 선택합니다.<br>• 이벤트 유형에서 Security Hub 조사 결과 - 가져오기를 선택합니다.<br>• (선택 사항)규칙을 더 구체적으로 만들려면 필터 값을 추가합니다. 예를 들어, 규칙을 활성 레코드 상태의 조사 결과로 제한하려면 특정 레코드 상태에 대해 활성을 선택합니다. | |

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
|---|---|---|
| 사용자 지정 이벤트 패턴입니다.<br><br>(EventBridge 콘솔에 표시되지 않은 속성을 기반으로 조사 결과를 필터링하려면 사용자 지정 패턴을 사용하세요.) | • 이벤트 패턴 섹션에서 사용자 지정 패턴(JSON 편집기)를 선택하고 다음 이벤트 패턴을 텍스트 영역에 붙여 넣습니다.<br><br>`{ "source": [ "aws.securityhub" ], "detail-type": [ "Security Hub Findings - Imported" ], "detail": { "findings": { "<attribute name> ": [ "<value1>", "<value2>"] } } }`<br><br>• 필터로 사용할 속성 및 속성 값을 포함하도록 이벤트 패턴을 업데이트합니다.<br><br>예를 들어, 확인 상태 `TRUE_POSITIVE` 인 조사 결과에 규칙을 적용하려면 다음 패턴 예제를 사용합니다. | |

| 다음을 사용하여 이벤트 패턴을 만들려면... | 수행할 작업 | |
|---|---|---|
| | <pre>{<br>  "source": [<br>  "aws.secu<br>rityhub"<br>  ],<br>  "detail-type": [<br>  "Security<br> Hub Findings -<br> Imported"<br>  ],<br>  "detail": {<br>  "findings": {<br>  "Verifica<br>tionState":<br> ["TRUE_POSITIVE"]<br>  }<br>  }<br>}</pre> | |

- 대상 유형에서 AWS 서비스를 선택하고 대상 선택에서 Amazon SNS 주제 또는 AWS Lambda 함수와 같은 대상을 선택합니다. 규칙에 정의된 이벤트 패턴과 일치하는 이벤트를 수신할 때 대상이 트리거됩니다.

규칙 생성에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 이벤트에 대응하는 Amazon EventBridge 규칙 생성를 참조하세요.

## 사용자 지정 작업을 사용하여 조사 결과 및 인사이트 조사 결과를 EventBridge로 전송

AWS Security Hub CSPM 사용자 지정 작업을 사용하여 조사 결과 또는 인사이트 결과를 Amazon EventBridge로 보내려면 먼저 Security Hub CSPM에서 사용자 지정 작업을 생성합니다. 그런 다음 사용자 지정 작업에 적용되는 규칙을 EventBridge에서 정의할 수 있습니다.

최대 50개의 사용자 지정 작업을 생성할 수 있습니다.

교차 리전 집계 활성화를 활성화하고 집계 영역의 조사 결과를 관리하는 경우, 집계 리전에서 사용자 지정 작업을 생성하세요.

EventBridge의 규칙은 사용자 지정 작업의 Amazon 리소스 이름(ARN)을 사용합니다.

### 사용자 지정 작업 생성

AWS Security Hub CSPM에서 사용자 지정 작업을 생성할 때 이름, 설명 및 고유 식별자를 지정합니다.

사용자 지정 작업은 EventBridge 이벤트가 EventBridge 규칙과 일치할 때 수행할 작업을 지정합니다. Security Hub CSPM은 각 조사 결과를 EventBridge에 이벤트로 전송합니다.

원하는 방법을 선택하고 다음 단계를 완료하여 사용자 지정 작업을 생성합니다.

#### Console

Security Hub CSPM에서 사용자 지정 작업을 생성하려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 설정을 선택한 다음 사용자 지정 작업를 선택합니다.
3. 사용자 지정 작업 생성을 선택하세요.
4. 작업에 대한 이름, 설명 및 사용자 지정 작업 ID를 입력하세요.

   이름은 20자 미만이어야 합니다.

   사용자 지정 작업 ID는 각 AWS 계정에 대해 고유해야 합니다.
5. 사용자 지정 작업 생성을 선택하세요.
6. 사용자 지정 작업 ARN을 기록해 둡니다. EventBridge에서 이 작업과 연결할 규칙을 생성할 때 ARN을 사용해야 합니다.

#### API

사용자 지정 작업을 생성하려면(API)

CreateActionTarget 작업을 사용합니다. 를 사용하는 경우 create-action-target 명령을 AWS CLI실행합니다.

다음 예제에서는 조사 결과를 문제 해결 도구로 보내는 사용자 지정 작업을 생성합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub create-action-target --name "Send to remediation" --description
 "Action to send the finding for remediation tracking" --id "Remediation"
```

EventBridge에서의 규칙 정의

Amazon EventBridge에서 사용자 지정 작업을 트리거하려면 EventBridge에서 해당 규칙을 생성해야 합니다. 규칙 정의에는 사용자 지정 작업의 Amazon 리소스 이름(ARN)이 포함됩니다.

Security Hub 조사 결과 - 사용자 지정 작업 이벤트의 이벤트 패턴은 다음과 같은 형식입니다.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Security Hub 인사이트 결과 이벤트의 이벤트 패턴은 다음과 같은 형식입니다.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

두 패턴 모두 *<custom action ARN>*이(가) 사용자 지정 작업의 ARN입니다. 둘 이상의 사용자 지정 작업에 적용되는 규칙을 구성할 수 있습니다.

여기에 제공된 지침은 EventBridge 콘솔을 위한 것입니다. 콘솔을 사용하면 EventBridge는 EventBridge가 CloudWatch Logs에 기록할 수 있도록 필요한 리소스 기반 정책을 자동으로 생성합니다.

EventBridge API의 `PutRule` API 작업을 사용할 수도 있습니다. 하지만 EventBridge API를 사용하는 경우, 리소스 기반 정책을 생성해야 합니다. 필수 정책에 대한 자세한 내용은 Amazon EventBridge 사용 설명서의 CloudWatch Logs 권한을 참조하세요.

EventBridge에서 규칙을 정의하려면(EventBridge 콘솔)

1. https://console.aws.amazon.com/events/에서 Amazon EventBridge 콘솔을 엽니다.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.
4. 규칙에 대해 이름과 설명을 입력하세요.
5. 이벤트 버스에서 이 규칙과 연결할 이벤트 버스를 선택합니다. 이 규칙이 자신의 계정에서 발생하는 이벤트와 일치하도록 하려면 기본을 선택합니다. 계정의 AWS 서비스가 이벤트를 출력하면 항상 계정의 기본 이벤트 버스로 이동합니다.
6. 규칙 유형에서 이벤트 패턴이 있는 규칙을 선택합니다.
7. 다음을 선택합니다.
8. 이벤트 소스에서 AWS 이벤트를 선택합니다.
9. 이벤트 패턴에서 이벤트 패턴 양식을 선택합니다.
10. 이벤트 소스에서 AWS 서비스를 선택합니다.
11. AWS 서비스를 받으려면 Security Hub를 선택합니다.
12. 이벤트 유형에서 다음 중 하나를 수행합니다.
    - 조사 결과를 사용자 지정 작업에 보낼 때 적용할 규칙을 생성하려면 Security Hub 조사 결과 - 사용자 지정 작업을 선택합니다.
    - 사용자 지정 작업에 인사이트 결과를 보낼 때 적용할 규칙을 생성하려면 Security Hub Insight 결과를 선택합니다.
13. 특정 사용자 지정 작업 ARN을 선택하고 사용자 지정 작업 ARN을 추가합니다.

    규칙이 여러 사용자 지정 작업에 적용되는 경우, 추가를 선택하여 사용자 지정 작업 ARN을 더 추가합니다.
14. 다음을 선택합니다.
15. 대상 선택에서 이 규칙이 일치할 때 간접적으로 호출할 대상을 선택하고 구상합니다.
16. 다음을 선택합니다.
17. (선택 사항)규칙에 대해 하나 이상의 태그를 입력하세요. 자세한 정보는 Amazon EventBridge 사용 설명서의 Amazon EventBridge 태그를 참조하세요.

18. 다음을 선택합니다.
19. 규칙의 세부 정보를 검토하고 규칙 생성을 선택합니다.

    계정의 조사 결과 또는 인사이트 조사 결과에 대해 사용자 지정 작업을 수행하면 EventBridge에서 이벤트가 생성됩니다.

조사 결과 및 인사이트 조사 결과에 대한 사용자 지정 작업 선택

AWS Security Hub CSPM 사용자 지정 작업 및 Amazon EventBridge 규칙을 생성한 후 자동 관리 및 처리를 위해 조사 결과 및 인사이트 결과를 EventBridge로 보낼 수 있습니다.

이벤트는 해당 이벤트가 표시된 계정의 EventBridge에만 전송됩니다. 관리자 계정을 사용하여 조사 결과를 보는 경우, 이벤트는 관리자 계정으로 EventBridge에 전송됩니다.

AWS API 호출이 유효하려면 대상 코드 구현이 역할을 멤버 계정으로 전환해야 합니다. 이는 전환해야 하는 역할을 작업이 필요한 각 구성원에게 배포해야 함을 의미합니다.

조사 결과를 EventBridge로 보내려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 조사 결과 목록 표시:
   - 조사 결과에서 활성화된 모든 제품 통합 및 제어의 조사 결과를 볼 수 있습니다.
   - 보안 표준에서는 선택한 제어에서 생성된 조사 결과 목록으로 이동할 수 있습니다. 자세한 내용은 Security Hub CSPM에서 제어 세부 정보 검토 섹션을 참조하세요.
   - 통합에서는 활성화된 통합에 의해 생성된 조사 결과 목록으로 이동할 수 있습니다. 자세한 내용은 Security Hub CSPM 통합에서 조사 결과 보기 섹션을 참조하세요.
   - 인사이트에서는 일치하는 인사이트 조사 결과에 대한 조사 결과 목록으로 이동할 수 있습니다. 자세한 내용은 Security Hub CSPM에서 인사이트 검토 및 조치 섹션을 참조하세요.
3. EventBridge로 전송할 조사 결과를 선택합니다. 한 번에 최대 20개 조사 결과까지 선택할 수 있습니다.
4. 작업에서 적용할 EventBridge 규칙과 일치하는 사용자 지정 작업을 선택하세요.

   Security Hub CSPM은 각 조사 결과에 대해 별도의 Security Hub CSPM 조사 결과 - 사용자 지정 작업 이벤트를 전송합니다.

인사이트 결과를 EventBridge로 보내려면(콘솔)

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 인사이트를 선택합니다.
3. 인사이트 페이지에서 EventBridge에 보낼 결과가 포함된 인사이트을 선택합니다.
4. EventBridge로 전송할 인사이트 결과를 선택합니다. 한 번에 최대 20개 결과까지 선택할 수 있습니다.
5. 작업에서 적용할 EventBridge 규칙과 일치하는 사용자 지정 작업을 선택하세요.

# Security Hub CSPM의 대시보드 작업

Security Hub CSPM 콘솔의 요약 대시보드에는 위험, 공격 시퀀스, 보안 적용 범위에 대한 요약이 표시됩니다. 이 대시보드는 다양한 보안 기능에 대한 심각도 및 계정 적용 범위를 기준으로 위험과 공격 시퀀스를 식별하는 데 도움이 됩니다. 대시보드는 열 때마다 자동으로 새로 고쳐집니다. 그러나 보안 점수 및 제어 상태는 24시간마다 새로 고쳐집니다.

다양한 보안 위젯을 추가 및 제거하여 요약 대시보드를 사용자 지정할 수 있습니다. 필터 기준을 지정하여 특정 유형의 데이터를 검색하고 표시할 수도 있습니다. 대시보드를 사용자 지정하면 Security Hub가 사용자 지정 설정을 저장합니다. 계정의 다른 사용자가 대시보드를 사용자 지정하면 변경 내용이 사용자 지정 설정과 독립적으로 저장됩니다.

Security Hub CSPM에서 교차 리전 집계를 구성한 경우 요약 대시보드에 집계된 데이터가 표시됩니다. 조직의 위임된 관리자 계정인 경우, 데이터에는 관리자 계정 및 멤버 계정에 대한 조사 결과가 포함됩니다. 멤버 계정 또는 독립형 계정인 경우, 데이터에는 해당 계정에 대한 조사 결과만 포함됩니다.

주제

- 요약 대시보드에 사용할 수 있는 위젯
- Security Hub CSPM의 요약 대시보드 필터링
- Security Hub CSPM의 요약 대시보드 사용자 지정

## 요약 대시보드에 사용할 수 있는 위젯

요약 대시보드에는 AWS 고객의 보안 운영 및 경험에 따라 최신 클라우드 보안 위협 환경을 반영하는 위젯이 포함되어 있습니다. 일부 위젯은 기본적으로 표시되지만 어떤 위젯은 표시되지 않습니다. 위젯을 추가하거나 제거하여 대시보드 보기를 사용자 지정할 수 있습니다.

위젯을 추가하려면 대시보드 상단에서 위젯 추가를 선택합니다. 그런 다음 사용 가능한 위젯의 목록을 찾아보거나 검색 창에 위젯의 제목을 입력할 수 있습니다. 추가할 위젯을 찾으면 대시보드에 표시할 위치로 드래그합니다. 자세한 내용은 대시보드 사용자 지정 단원을 참조하십시오.

## 위젯은 기본적으로 표시

기본적으로 요약 대시보드에는 다음 위젯이 포함됩니다.

상위 위협 시퀀스

심각도가 가장 높은 위협 시퀀스를 표시합니다. Amazon GuardDuty에서 공격 시퀀스 조사 결과라고 하는 위협 시퀀스 조사 결과는 여러 이벤트의 상관관계를 파악하여 AWS 환경에 대한 잠재적 위협을 식별합니다. 위협 시퀀스에는 환경에서 진행 중이거나 최근(24시간 이내)의 공격 동작이 포함될 수 있으며, 이로 인해 추가 침해가 발생할 수 있습니다. Security Hub CSPM에서 위협 시퀀스 조사 결과를 수신하려면 GuardDuty 및 GuardDuty S3 보호가 활성화되어 있어야 합니다.

상위 위험

환경의 주요 위험에 대한 요약을 표시합니다. 위젯 상단에는 각 심각도 수준의 위험 수가 표시됩니다. 심각도 수준을 선택하여 선택한 심각도 수준으로 필터링된 위험이 표시된 위험 페이지로 이동할 수 있습니다. 환경에서 가장 많이 발생하는 위험이 먼저 표시됩니다. 이 위젯은 완화할 위험의 우선순위를 정하는 데 도움이 됩니다.

보안 적용 범위

적용 범위 제어 조사 결과를 기반으로 보안 적용 범위를 요약합니다. 적용 범위 제어는 특정 AWS 서비스 및 해당 기능이 활성화되어 있는지 확인합니다(예: [Macie.1] Amazon Macie가 활성화되어야 합니다.). 이 위젯은 적용 범위 제어에 대한 PASSED 조사 결과가 있는지 확인하는 데 도움이 됩니다. Security Hub CSPM 콘솔은 누락된 보안 기능을 활성화하는 데 도움이 되도록 이 위젯의 링크를 제공합니다. 여러 AWS 계정 및에서 누락된 보안 기능을 활성화하려면 중앙 구성을 사용하는 것이 좋습니다 AWS 리전. 자세한 내용은 Security Hub CSPM의 중앙 구성 이해 단원을 참조하십시오.

보안 표준

가장 최근의 요약 보안 점수와 각 Security Hub CSPM 표준에 대한 보안 점수를 표시합니다. 0~100% 범위의 보안 점수는 활성화된 모든 제어와 비교하여 통과된 제어의 비율을 나타냅니다. 이러한 점수에 대한 자세한 내용은 보안 점수 계산 방법 섹션을 참조하세요. 이 위젯은 전반적인 보안 태세를 이해하는 데 도움이 됩니다.

가장 많은 조사 결과가 포함된 자산

가장 많은 조사 결과가 포함된 리소스, 계정 및 애플리케이션에 대한 개요를 제공합니다. 목록은 조사 결과 수를 기준으로 내림차순으로 정렬됩니다. 위젯의 각 탭은 해당 범주의 상위 6개 항목을 심각도 및 리소스 유형별로 그룹화하여 표시합니다. 전체 조사 결과 열에서 숫자를 선택하면 Security Hub CSPM에서 자산에 대한 조사 결과를 보여주는 페이지가 열립니다. 이 위젯을 사용하면 핵심 자산 중 잠재적 보안 위협이 있는 자산을 신속하게 식별할 수 있습니다.

리전별 조사 결과

Security Hub CSPM이 활성화된 각 AWS 리전 에서 심각도별로 그룹화한 조사 결과의 총 수를 표시합니다. 이 위젯은 특정 리전에 영향을 미칠 수 있는 보안 문제를 식별하는 데 도움이 됩니다. 집계 영역에서 대시보드를 여는 경우, 이 위젯을 통해 연결된 각 리전의 잠재적 보안 문제를 모니터링할 수 있습니다.

가장 일반적인 위협 유형

AWS 환경에서 가장 일반적인 10가지 유형의 위협에 대한 분석을 제공합니다. 여기에는 권한 에스컬레이션, 노출된 보안 인증 사용 또는 악의적인 IP 주소와의 통신과 같은 위협이 포함됩니다.

이 데이터를 보려면 Amazon GuardDuty를 활성화해야 합니다. 활성화되면 이 위젯에서 위협 유형을 선택하여 GuardDuty 콘솔을 열고 이 위협과 관련된 조사 결과를 검토하세요. 이 위젯은 다른 보안 문제의 컨텍스트에서 잠재적 위협을 평가하는 데 도움이 됩니다.

악용을 통한 소프트웨어 취약성

AWS 환경에 존재하고 알려진 악용이 있는 소프트웨어 취약성에 대한 요약을 제공합니다. 또한 수정 사항을 사용할 수 있는 취약성과 사용할 수 없는 취약성을 분류하여 검토할 수 있습니다.

이 데이터를 보려면 Amazon Inspector를 활성화해야 합니다. 활성화되면 이 위젯에서 통계를 선택하여 Amazon Inspector 콘솔을 열고 취약성에 대한 자세한 내용을 검토하세요. 이 위젯은 다른 보안 문제의 컨텍스트에서 소프트웨어 취약성을 평가하는 데 도움이 됩니다.

시간 경과에 따른 새로운 조사 결과

지난 90일 동안의 새로운 일일 조사 결과 수의 추세를 보여줍니다. 추가 컨텍스트를 위해 심각도 또는 공급자별로 데이터를 분류할 수 있습니다. 이 위젯을 사용하면 지난 90일 동안 특정 시간에 조사 결과 볼륨이 급증하거나 감소했는지 파악할 수 있습니다.

가장 많은 조사 결과가 포함된 리소스

Amazon Simple Storage Service(Amazon S3 Amazon EC2) 인스턴스 및 AWS Lambda 함수와 같은 리소스 유형별로 분류하여 가장 많은 결과를 생성한 리소스에 대한 요약을 제공합니다.

위젯의 각 탭은 이전 리소스 유형 중 하나에 초점을 맞추어 가장 많은 조사 결과를 생성한 10개의 리소스 인스턴스를 나열합니다. 특정 리소스에 대한 조사 결과를 검토하려면 리소스 인스턴스를 선택합니다. 이 위젯은 공통 AWS 리소스와 관련된 보안 조사 결과를 분류하는 데 도움이 됩니다.

## 위젯은 기본적으로 숨김

다음 위젯은 요약 대시보드에서도 사용할 수 있지만 기본적으로 숨깁니다.

가장 많은 조사 결과가 포함된 AMI

가장 많은 조사 결과를 생성한 Amazon Machine Image(AMI) 10개의 목록을 제공합니다. 이 데이터는 사용자 계정에 대해 Amazon EC2가 활성화된 경우에만 사용할 수 있습니다. 이를 통해 잠재적 보안 위험을 야기하는 AMI를 식별할 수 있습니다.

가장 많은 조사 결과가 포함된 IAM 보안 주체

가장 많은 조사 결과를 생성한 10 AWS Identity and Access Management (IAM)명의 사용자 목록을 제공합니다. 이 위젯은 관리 및 결제 작업을 수행하는 데 도움이 됩니다. Security Hub CSPM 사용에 가장 많이 기여하는 사용자를 보여줍니다.

가장 많은 조사 결과가 포함된 계정(심각도별)

가장 많은 조사 결과를 생성한 10개 계정을 심각도별로 그룹화하여 그래프로 표시합니다. 이 위젯은 분석 및 문제 해결 노력을 집중할 계정을 결정하는 데 도움이 됩니다.

가장 많은 조사 결과가 포함된 계정(리소스 유형별)

가장 많은 조사 결과를 생성한 10개 계정을 리소스 유형별로 그룹화여 그래프로 표시합니다. 이 위젯은 분석 및 문제 해결을 위해 우선적으로 지정할 계정 및 리소스 유형을 결정하는 데 도움이 됩니다.

인사이트

5개 Security Hub CSPM 관리형 인사이트와 이를 통해 생성된 조사 결과 수를 나열합니다. 인사이트는 주의가 필요한 특정 보안 영역을 식별합니다.

AWS 통합의 최신 결과

통합 AWS 서비스에서 Security Hub CSPM으로 수신한 조사 결과 수를 표시합니다. 또한 각 통합 서비스에서 가장 최근에 조사 결과를 받은 시기도 표시합니다. 이 위젯은 여러의 통합 결과 데이터를 제공합니다 AWS 서비스. 자세히 살펴보려면 통합 서비스를 선택합니다. 그런 다음 Security Hub CSPM에서 해당 서비스의 콘솔을 엽니다.

# Security Hub CSPM의 요약 대시보드 필터링

Security Hub CSPM 콘솔의 요약 대시보드를 큐레이션하여 가장 관련성이 높은 보안 데이터만 포함하도록 할 수 있습니다. 예를 들어, 애플리케이션 팀의 팀원인 경우, 프로덕션 환경의 중요한 애플리케이션에 대한 전용 보기를 만들 수 있습니다. 보안 팀의 팀원인 경우, 심각도가 높은 조사 결과에 집중하는 데 도움이 되는 전용 보기를 만들 수 있습니다.

이러한 큐레이션된 뷰를 생성하려면 대시보드 위의 필터 상자에 필터 기준을 입력합니다. 필터 기준을 적용하면 인사이트 및 보안 표준 위젯의 데이터를 제외한 대시보드의 모든 데이터와 위젯에 기준이 적용됩니다. 대시보드에서 사용 가능한 위젯 목록은 요약 대시보드에 사용할 수 있는 위젯 섹션을 참조하세요.

다음 필드를 사용하여 데이터를 필터링할 수 있습니다.

- 계정 이름
- 계정 ID
- 애플리케이션 ARN
- 애플리케이션 이름
- 제품 이름( Security Hub CSPM으로 조사 결과를 보내는 AWS 서비스 또는 타사 제품의 경우)
- 레코드 상태
- 리전
- 리소스 태그
- 심각도
- 워크플로 상태

기본적으로 대시보드 데이터는 다음 기준을 사용하여 필터링합니다. `Workflow.Status`은(는) `NOTIFIED` 또는 `NEW`이고, `RecordState`은(는) `ACTIVE`입니다. 이러한 기준은 대시보드 위, 필터 상자 아래에 표시됩니다. 이러한 기준을 제거하려면 제거하려는 기준에 대한 필터 토큰에서 X를 선택합니다.

다시 사용하려는 필터를 적용하는 경우, 해당 내용을 필터 세트로 저장할 수 있습니다. 필터 세트는 요약 대시보드에서 데이터를 결과를 검토할 때 다시 적용하기 위해 만들고 저장하는 필터 기준 세트입니다. 애플리케이션 ARN, 애플리케이션 이름, 리소스 태그를 제외한 사용 가능한 필드를 사용하는 필터 세트를 생성하고 저장할 수 있습니다.

## 필터 세트 생성 및 저장

필드 세트를 만들려면 다음 단계를 따르세요.

필터 세트를 만들고 저장하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다.
3. 요약 대시보드 위의 필터 상자에 필터 세트의 필터 기준을 입력합니다.
4. 필터 지우기 메뉴에서 새로운 필터 세트 저장을 선택합니다.
5. 필터 세트 저장 대화 상자에 필터 세트 이름을 입력합니다.
6. (선택 사항)요약 페이지를 열 때마다 기본적으로 필터 세트를 사용하려면 해당 필터 세트를 기본 보기로 설정하는 옵션을 선택합니다.
7. 저장을 선택합니다.

만들고 저장한 필터 세트 간에 전환하려면 요약 대시보드 위의 필터 세트 선택 메뉴를 사용합니다. 필터 세트를 선택하면 Security Hub CSPM은 필터 세트의 기준을 대시보드의 데이터에 적용합니다.

## 필터 세트 업데이트 또는 삭제

기존 필터 세트를 업데이트하거나 삭제하려면 다음 단계를 따르세요. 현재 요약 대시보드의 기본 보기로 설정된 필터 세트를 삭제하면 기본 보기가 기본 Security Hub CSPM 보기로 재설정됩니다.

필터 세트를 업데이트 또는 삭제하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다.
3. 요약 페이지 위의 필터 세트 선택 메뉴에서 필터 세트를 선택합니다.
4. 필터 지우기 메뉴에서 다음 중 하나를 수행합니다.
   - 필터 세트를 업데이트하려면 현재 필터 세트 업데이트를 선택합니다. 그런 다음 나타나는 대화 상자에 변경 사항을 입력합니다.
   - 필터 세트를 삭제하려면 현재 필터 세트 삭제를 선택합니다. 그런 다음 나타나는 대화 상자에서 삭제를 선택합니다.

## Security Hub CSPM의 요약 대시보드 사용자 지정

여러 가지 방법으로 Security Hub CSPM 콘솔의 요약 대시보드를 사용자 지정할 수 있습니다. 예를 들어, 대시보드에서 위젯을 추가하거나 제거할 수 있습니다. 대시보드에서 위젯을 재배열하고 크기를 조정할 수도 있습니다. 사용 가능한 위젯의 목록 및 각 위젯에 대한 설명은 요약 대시보드에 사용할 수 있는 위젯 섹션을 참조하세요.

대시보드를 사용자 지정하는 경우, Security Hub CSPM은 변경 사항을 즉시 적용하고 새로운 대시보드 설정을 저장합니다. 변경 사항은 모든 AWS 리전 및 브라우저의 대시보드 보기에 적용됩니다.

요약 대시보드를 사용자 지정하려면

1. https://console.aws.amazon.com/securityhub/ AWS Security Hub CSPM 콘솔을 엽니다.
2. 탐색 창에서 요약을 선택합니다.
3. 해결 방법:

   - 위젯을 추가하려면 페이지의 오른쪽 상단에서 위젯 추가를 선택합니다. 검색창에 추가할 위젯의 제목을 입력합니다. 그런 다음 위젯을 원하는 위치로 끌어다 놓습니다.
   - 위젯을 제거하려면 위젯의 오른쪽 상단 모서리에 있는 3개의 점을 선택합니다.
   - 위젯을 이동하려면 위젯의 왼쪽 상단 모서리에 있는 핸들을 선택한 다음 위젯을 원하는 위치로 끌어다 놓습니다.
   - 위젯의 크기를 변경하려면 위젯의 오른쪽 하단 모서리에 있는 크기 조정 핸들을 선택합니다. 위젯이 원하는 크기가 될 때까지 위젯의 가장자리를 끌어다 놓습니다.

이후에 원래 설정을 복원하려면 페이지의 상단에서 기본 레이아웃으로 리셋을 선택합니다.

# Security Hub CSPM 리전 제한

일부 AWSSecurity Hub CSPM 기능은 특정 에서만 사용할 수 있습니다AWS 리전. 다음 섹션에서는 이러한 리전별 제한을 지정합니다. 현재 Security Hub CSPM을 사용할 수 있는 모든 리전의 목록은 AWS 일반 참조의 AWS Security Hub CSPM 엔드포인트 및 할당량을 참조하세요.

## 교차 리전 집계 제한

에서는의 조사 결과AWS GovCloud (US) Regions, 조사 결과 업데이트 및 인사이트AWS GovCloud (US) Regions에만 교차 리전 집계를 사용할 수 있습니다. 특히 조사 결과, 조사 결과 업데이트 및 인사이트는 AWSGovCloud(미국 동부)와 AWSGovCloud(미국 서부) 리전 간에만 집계할 수 있습니다.

중국 리전에서는 중국 리전 전반에 대해서만 조사 결과, 조사 결과 업데이트, 인사이트에 대해 교차 리전 집계를 사용할 수 있습니다. 특히 중국(베이징) 리전과 중국(닝샤) 리전 간에는 조사 결과, 조사 결과 업데이트, 인사이트만 집계할 수 있습니다.

기본적으로 비활성화된 리전은 집계 영역으로 사용할 수 없습니다. 기본적으로 비활성화된 리전 목록은 AWS Account Management참조 안내서의 계정AWS 리전에서 활성화 또는 비활성화를 참조하세요.

## 리전별 통합 사용 가능 여부

일부 통합은 전혀 사용할 수 없습니다AWS 리전. Security Hub CSPM 콘솔에서 현재 로그인한 리전에서 지원되지 않는 통합은 통합 페이지에 표시되지 않습니다.

### 중국(베이징) 및 중국(닝샤) 리전에서 지원되는 통합

중국(베이징) 및 중국(닝샤) 리전에서는 다음과 같은 AWS 서비스와의 통합만 지원합니다.

- 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 Manager패치 관리자

중국(베이징) 및 중국(닝샤) 리전에서는 다음과 같은 서드 파티 통합만 지원합니다.

- 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

## AWS GovCloud (US-East)및 AWS GovCloud (US-West)리전에서 지원되는 통합

AWS GovCloud (US-East)및 AWS GovCloud (US-West)리전에서 Security Hub CSPM은 와의 다음 통합AWS 서비스만 지원합니다.

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health
- IAM Access Analyzer
- Amazon Inspector –
- AWS IoT Device Defender

AWS GovCloud (US-East)및 AWS GovCloud (US-West)리전에서 Security Hub CSPM은 다음과 같은 타사 통합만 지원합니다.

- 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(AWS GovCloud(미국 서부)에서만 사용 가능)
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

## 리전별 표준 사용 가능 여부

AWS Control Tower 서비스 관리형 표준은가 AWS 리전지원하는AWS Control Tower 에서만 사용할 수 있습니다. AWS Control Tower현재가 지원하는 리전 목록은 AWS Control Tower사용 설명서의 AWS 리전작업 방식을 AWS Control Tower 참조하세요.

아시아 태평양(타이베이) 리전에서는 AWS리소스 태그 지정 표준을 사용할 수 없습니다.

기타 보안 표준은 현재 Security Hub CSPM이 제공되는 모든 리전에서 사용할 수 있습니다.

## 리전별 제어 기능 사용 가능 여부

일부 Security Hub CSPM 제어는 전혀 사용할 수 없습니다AWS 리전. 각 리전에서 사용할 수 없는 제어의 목록은 Security Hub CSPM 제어에 대한 리전별 제한 섹션을 참조하세요.

현재 로그인한 리전에서 사용할 수 없는 제어는 Security Hub CSPM 콘솔의 제어 목록에 표시되지 않습니다. 집계 영역은 예외입니다. 집계 영역을 설정하고 해당 리전에 로그인한 경우 콘솔에 집계 영역 또는 하나 이상의 연결된 리전에서 사용할 수 있는 제어가 표시됩니다.

## Security Hub CSPM 제어에 대한 리전별 제한

일부 AWS Security Hub CSPM 제어는 전혀 사용할 수 없습니다 AWS 리전. 이 페이지에서는 특정 리전에서 사용할 수 없는 제어를 보여줍니다.

현재 로그인한 리전에서 사용할 수 없는 제어는 Security Hub CSPM 콘솔의 제어 목록에 표시되지 않습니다. 집계 영역은 예외입니다. 집계 영역을 설정하고 해당 리전에 로그인한 경우 콘솔에 집계 영역 또는 하나 이상의 연결된 리전에서 사용할 수 있는 제어가 표시됩니다.

AWS 리전

- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)
- 아프리카(케이프타운)
- 아시아 태평양(홍콩)
- 아시아 태평양(하이데라바드)
- 아시아 태평양(자카르타)
- 아시아 태평양(말레이시아)
- 아시아 태평양(멜버른)
- 아시아 태평양(뭄바이)
- 아시아 태평양(뉴질랜드)
- 아시아 태평양(오사카)
- 아시아 태평양(서울)
- 아시아 태평양(싱가포르)
- 아시아 태평양(시드니)
- 아시아 태평양(타이베이)
- 아시아 태평양(태국)

- 아시아 태평양(도쿄)
- 캐나다(중부)
- 캐나다 서부(캘거리)
- 중국(베이징)
- 중국(닝샤)
- 유럽(프랑크푸르트)
- 유럽(아일랜드)
- 유럽(런던)
- 유럽(밀라노)
- 유럽(파리)
- 유럽(스페인)
- 유럽(스톡홀름)
- 유럽(취리히)
- 이스라엘(텔아비브)
- 멕시코(중부)
- Middle East (Bahrain)
- 중동(UAE)
- 남아메리카(상파울루)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

## 미국 동부(버지니아 북부)

다음 제어는 미국 동부(버지니아 북부) 리전에서 지원되지 않습니다.

- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.

- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다

## 미국 동부(오하이오)

다음 제어는 미국 동부(오하이오) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다

- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 미국 서부(캘리포니아 북부)

다음 제어는 미국 서부(캘리포니아 북부) 리전에서 지원되지 않습니다.

- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.

- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.

- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 미국 서부(오리건)

다음 제어는 미국 서부(오리건) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.

- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 아프리카(케이프타운)

다음 제어는 아프리카(케이프타운) 리전에서 지원되지 않습니다.

- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다

- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.

- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.

- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 아시아 태평양(홍콩)

다음 제어는 아시아 태평양(홍콩) 리전에서 지원되지 않습니다.

- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.

- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다

- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.

- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(하이데라바드)

다음 제어는 아시아 태평양(하이데라바드) 리전에서 지원되지 않습니다.

- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.

- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.

- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다

- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.

- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다

- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.

- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다

- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(자카르타)

다음 제어는 아시아 태평양(자카르타) 리전에서 지원되지 않습니다.

- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.

- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.

- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다

- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.

- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.

- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.

- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(말레이시아)

다음 제어는 아시아 태평양(말레이시아) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.

- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.2]AWS Backup복구 지점에 태그를 지정해야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.

- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.

- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.

- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.

- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.

- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [ECS.19] ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.
- [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다

- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [ES.9] Elasticsearch 도메인에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.

- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.
- [FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.1]AWS Glue작업에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.

- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.

- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.

- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.

- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다

- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다

- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다

- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(멜버른)

다음 제어는 아시아 태평양(멜버른) 리전에서 지원되지 않습니다.

- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.

- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.

- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.

- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.

- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.

- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다

- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(뭄바이)

다음 제어는 아시아 태평양(뭄바이) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.

- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다

- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 아시아 태평양(뉴질랜드)

다음 제어는 아시아 태평양(뉴질랜드) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.

- [APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.4]AWS AppSyncGraphQL APIs 태그를 지정해야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Athena.2] Athena 데이터 카탈로그에 태그를 지정해야 합니다.
- [Athena.3] Athena 작업 그룹에 태그를 지정해야 합니다.
- [Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.2]AWS Backup복구 지점에 태그를 지정해야 합니다.

- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.

- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.

- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.

- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.172] EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다

- [EC2.182] Amazon EBS 스냅샷에 대해 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [ECS.18] ECS 작업 정의는 EFS 볼륨에 대해 전송 중 암호화를 사용해야 합니다.
- [ECS.19] ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다.
- [ECS.20] ECS 작업 정의는 Linux 컨테이너 정의에서 루트가 아닌 사용자를 구성해야 합니다.
- [ECS.21] ECS 작업 정의는 Windows 컨테이너 정의에서 관리자가 아닌 사용자를 구성해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.
- [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.

- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] Application Load Balancer는 AWS WAF 웹 ACL과 연결되어야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.
- [ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.

- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [ES.9] Elasticsearch 도메인에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.
- [FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.1]AWS Glue작업에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.1] GuardDuty를 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.

- [GuardDuty.3] GuardDuty IPSets에 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.

- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.

- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.

- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.

- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.

- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.

- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.1] Amazon EC2 인스턴스는에서 관리해야 합니다.AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [Transfer.1]AWS Transfer Family워크플로에 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.

- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11]AWS WAF웹 ACL 로깅을 활성화해야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(오사카)

다음 제어는 아시아 태평양(오사카) 리전에서 지원되지 않습니다.

- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.

- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.

- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다

- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다

- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.

- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(서울)

다음 제어는 아시아 태평양(서울) 리전에서 지원되지 않습니다.

- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.

- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 아시아 태평양(싱가포르)

다음 제어는 아시아 태평양(싱가포르) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다

- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 아시아 태평양(시드니)

다음 제어는 아시아 태평양(시드니) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.

- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 아시아 태평양(타이베이)

다음 제어는 아시아 태평양(타이베이) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [ACM.3] ACM 인증서에 태그를 지정해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.1] API Gateway REST 및 WebSocket API 실행 로깅이 활성화되어야 합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.3] API Gateway REST API 스테이지에는 AWS X-Ray 추적이 활성화되어 있어야 합니다.
- [APIGateway.4] API 게이트웨이는 WAF 웹 ACL과 연결되어야 합니다.
- [APIGateway.5] API Gateway REST API 캐시 데이터는 저장 시 암호화되어야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다

- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.4]AWS AppSyncGraphQL APIs 태그를 지정해야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Athena.2] Athena 데이터 카탈로그에 태그를 지정해야 합니다.
- [Athena.3] Athena 작업 그룹에 태그를 지정해야 합니다.
- [Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.
- [PCI.AutoScaling.1] 로드 밸런서와 연결된 Auto Scaling 그룹은 ELB 상태 확인을 사용해야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [AutoScaling.10] EC2 Auto Scaling 그룹에 태그를 지정해야 합니다.
- [Autoscaling.5] Auto Scaling 그룹 시작 구성을 사용하여 시작된 Amazon EC2 인스턴스에는 퍼블릭 IP 주소가 없어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.2]AWS Backup복구 지점에 태그를 지정해야 합니다.
- [Backup.3] AWS Backup볼트에 태그를 지정해야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Backup.5]AWS Backup백업 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.

- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.2] CloudFormation 스택에 태그를 지정해야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.

- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CloudTrail.9] CloudTrail 추적에는 태그를 지정해야 합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다

- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.1] Database Migration Service 복제 인스턴스는 공개되어서는 안 됩니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.5] DynamoDB 테이블에 태그를 지정해야 합니다.
- [DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.10] Amazon EC2는 Amazon EC2 서비스용으로 생성된 VPC 엔드포인트를 사용하도록 구성해야 합니다.

- [EC2.19] 보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.33] EC2 Transit Gateway Attachment에 태그를 지정해야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.35] EC2 네트워크 인터페이스에 태그를 지정해야 합니다.
- [EC2.36] EC2 고객 게이트웨이에 태그를 지정해야 합니다.
- [EC2.37] EC2 탄력적 IP 주소에 태그를 지정해야 합니다.
- [EC2.38] EC2 인스턴스에 태그를 지정해야 합니다.
- [EC2.39] EC2 인터넷 게이트웨이에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.41] EC2 네트워크 ACL에 태그를 지정해야 합니다.
- [EC2.42] EC2 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.43] EC2 보안 그룹에 태그를 지정해야 합니다.
- [EC2.44] EC2 서브넷에 태그를 지정해야 합니다.
- [EC2.45] EC2 볼륨에 태그를 지정해야 합니다.
- [EC2.46] Amazon VPC에 태그를 지정해야 합니다.
- [EC2.47] Amazon VPC 엔드포인트 서비스에 태그를 지정해야 합니다.
- [EC2.48] Amazon VPC 흐름 로그에 태그를 지정해야 합니다.
- [EC2.49] Amazon VPC 피어링 연결에 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.52] EC2 전송 게이트웨이에 태그를 지정해야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다

- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.172] EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.182] Amazon EBS 스냅샷에 대해 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.2] ECS 서비스에 퍼블릭 IP 주소가 자동으로 할당되어서는 안 됩니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.

- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.13] ECS 서비스에 태그를 지정해야 합니다
- [ECS.14] ECS 클러스터에 태그를 지정해야 합니다.
- [ECS.15] ECS 작업 정의에 태그를 지정해야 합니다.
- [ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [ECS.18] ECS 작업 정의는 EFS 볼륨에 대해 전송 중 암호화를 사용해야 합니다.
- [ECS.19] ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다.
- [ECS.20] ECS 작업 정의는 Linux 컨테이너 정의에서 루트가 아닌 사용자를 구성해야 합니다.
- [ECS.21] ECS 작업 정의는 Windows 컨테이너 정의에서 관리자가 아닌 사용자를 구성해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS .5] EFS 액세스 포인트에 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.
- [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.
- [EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [EKS.6] EKS 클러스터에 태그를 지정해야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.

- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.3] Classic Load Balancer 리스너는 HTTPS 또는 TLS 종료로 구성되어야 합니다.
- [ELB.7] Classic Load Balancer connection draining닝이 활성화되어 있어야 합니다.
- [ELB.8] SSL AWS Config리스너가 있는 Classic Load Balancer는 강력한 요구 사항이 있는 사전 정의된 보안 정책을 사용해야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.16] Application Load Balancer는 AWS WAF 웹 ACL과 연결되어야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.
- [ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.

- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.1] Elasticsearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [ES.2] Elasticsearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [ES.5] Elasticsearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [ES.6] Elasticsearch 도메인에는 최소 세 개의 데이터 노드가 있어야 합니다.
- [ES.7] Elasticsearch 도메인은 최소 3개의 전용 프라이머리 노드로 구성해야 합니다.
- [ES.8] Elasticsearch 도메인에 대한 연결은 TLS 보안 정책을 사용하여 암호화해야 합니다.
- [ES.9] Elasticsearch 도메인에 태그를 지정해야 합니다.
- [EventBridge.2] EventBridge 이벤트 버스에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.

- [FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.1]AWS Glue작업에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.1] GuardDuty를 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPSets에 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.

- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.23] IAM Access Analyzer 분석기에 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.

- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.2] Kinesis 스트림에 태그를 지정해야 합니다.
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.3] 실수로 삭제해서는 AWS KMS keys안 됩니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.6] Lambda 함수에는 태그를 지정해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.

- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.7] 네트워크 방화벽에 태그를 지정해야 합니다.
- [NetworkFirewall.8] 네트워크 방화벽 정책에 태그를 지정해야 합니다.

- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.16] Aurora DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.17] RDS DB 인스턴스는 태그를 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.19] 중요한 클러스터 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.20] 중요한 데이터베이스 인스턴스 이벤트에 대해 기존 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.21] 중요한 데이터베이스 파라미터 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.22] 중요한 데이터베이스 보안 그룹 이벤트에 대해 RDS 이벤트 알림 구독을 구성해야 합니다.
- [RDS.23] RDS 인스턴스는 데이터베이스 엔진 기본 포트를 사용하지 않아야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.

- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에 태그를 지정해야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에 태그를 지정해야 합니다.
- [RDS.30] RDS DB 인스턴스에 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.32] RDS DB 스냅샷에 태그를 지정해야 합니다.
- [RDS.33] RDS DB 서브넷 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.
- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에 태그를 지정해야 합니다.
- [Redshift.12] Redshift 이벤트 알림 구독에 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에 태그를 지정해야 합니다.
- [Redshift.14] Redshift 클러스터 서브넷 그룹에 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다

- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys
- [S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.

- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SecretsManager.1] Secrets Manager 암호에는 자동 교체가 활성화되어 있어야 합니다.
- [SecretsManager.2] 자동 교체로 구성된 Secrets Manager 암호는 성공적으로 교체되어야 합니다.
- [SecretsManager.3] 사용하지 않는 Secrets Manager 암호 삭제
- [SecretsManager.4] Secrets Manager 암호는 지정된 일수 내에 교체되어야 합니다.
- [SecretsManager.5] Secrets Manager 보안 암호에 태그를 지정해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SNS.3] SNS 주제에 태그를 지정해야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.1] Amazon EC2 인스턴스는에서 관리해야 합니다.AWS Systems Manager
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.

- [Transfer.1]AWS Transfer Family워크플로에 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.11]AWS WAF웹 ACL 로깅을 활성화해야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(태국)

다음 제어는 아시아 태평양(태국) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.

- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Athena.2] Athena 데이터 카탈로그에 태그를 지정해야 합니다.
- [Athena.3] Athena 작업 그룹에 태그를 지정해야 합니다.
- [Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.2]AWS Backup복구 지점에 태그를 지정해야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다

- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.

- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.

- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.172] EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.182] Amazon EBS 스냅샷에 대해 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.

- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [ECS.18] ECS 작업 정의는 EFS 볼륨에 대해 전송 중 암호화를 사용해야 합니다.
- [ECS.19] ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다.
- [ECS.20] ECS 작업 정의는 Linux 컨테이너 정의에서 루트가 아닌 사용자를 구성해야 합니다.
- [ECS.21] ECS 작업 정의는 Windows 컨테이너 정의에서 관리자가 아닌 사용자를 구성해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.
- [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.

- [EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [ES.9] Elasticsearch 도메인에 태그를 지정해야 합니다.

- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.
- [FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.1]AWS Glue작업에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.1] GuardDuty를 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.

- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.

- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.

- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다

- [RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.

- [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.

- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [Transfer.1]AWS Transfer Family워크플로에 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다

- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 아시아 태평양(도쿄)

다음 제어는 아시아 태평양(도쿄) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 캐나다(중부)

다음 제어는 캐나다(중부) 리전에서 지원되지 않습니다.

- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다

- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.

- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 캐나다 서부(캘거리)

다음 제어는 캐나다 서부(캘거리) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.

- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.

- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.

- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.

- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.

- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.
- [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다

- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.
- [FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다

- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.

- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.

- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다

- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.

- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다

- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다

- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.

- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 중국(베이징)

다음 제어는 중국(베이징) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.

- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.

- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.20] a AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.36] EC2 고객 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다

- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.
- [ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다

- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [GuardDuty.3] GuardDuty IPSets에 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.23] IAM Access Analyzer 분석기에 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.

- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.

- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.7] RDS 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [RDS.12] RDS 클러스터에 대해 IAM 인증을 구성해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.16] Aurora DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.

- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.28] RDS DB 클러스터에 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.

- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다

- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 중국(닝샤)

다음 제어는 중국(닝샤) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.

- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다

- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.20] a AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다.

- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.36] EC2 고객 게이트웨이에 태그를 지정해야 합니다.
- [EC2.50] EC2 VPN 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다

- [ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.
- [ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [GuardDuty.3] GuardDuty IPSets에 태그를 지정해야 합니다.
- [GuardDuty.4] GuardDuty 탐지기에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다

- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.23] IAM Access Analyzer 분석기에 태그를 지정해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다

- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
- [Lambda.2] Lambda 함수는 지원되는 런타임을 사용해야 합니다.
- [Lambda.3] Lambda 함수는 VPC에 있어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.6] Lambda 함수에는 태그를 지정해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.

- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.

- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다

- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 유럽(프랑크푸르트)

다음 제어는 유럽(프랑크푸르트) 리전에서 지원되지 않습니다.

- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.

- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 유럽(아일랜드)

다음 제어는 유럽(아일랜드) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 유럽(런던)

다음 제어는 유럽(런던) 리전에서 지원되지 않습니다.

- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다

- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## 유럽(밀라노)

다음 제어는 유럽(밀라노) 리전에서 지원되지 않습니다.

- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.

- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다

- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.

- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SSM.2] Systems Manager가 관리하는 Amazon EC2 인스턴스는 패치 설치 후 패치 규정 준수 상태가 COMPLIANT여야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 유럽(파리)

다음 제어는 유럽(파리) 리전에서 지원되지 않습니다.

- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.

- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.

- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 유럽(스페인)

다음 제어는 유럽(스페인) 리전에서 지원되지 않습니다.

- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.

- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.

- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.1] Amazon EBS 스냅샷은 공개적으로 복원 가능하도록 구성해서는 안 됩니다.
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.

- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.

- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.1] Lambda 함수 정책은 퍼블릭 액세스를 금지해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다

- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다

- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다

- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 유럽(스톡홀름)

다음 제어는 유럽(스톡홀름) 리전에서 지원되지 않습니다.

- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.

- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다

- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 유럽(취리히)

다음 제어는 유럽(취리히) 리전에서 지원되지 않습니다.

- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.

- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다

- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.

- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.

- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.

- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다

- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.

- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다

- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 이스라엘(텔아비브)

다음 제어는 이스라엘(텔아비브) 리전에서 지원되지 않습니다.

- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다

- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다

- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.

- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys

- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.2] SSL/HTTPS 리스너가 있는 Classic Load Balancer는에서 제공하는 인증서를 사용해야 합니다. AWS Certificate Manager
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.

- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.
- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.

- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.

- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [RDS.1] RDS 스냅샷은 비공개여야 합니다.
- [RDS.4] RDS 클러스터 스냅샷과 데이터베이스 스냅샷은 저장 시 암호화되어야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.29] RDS DB 클러스터 스냅샷에 태그를 지정해야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.

- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.

- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 멕시코(중부)

다음 제어는 멕시코(중부) 리전에서 지원되지 않습니다.

- [ACM.1] 가져온 인증서와 ACM에서 발급한 인증서는 지정된 기간 후에 갱신해야 합니다.
- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.4]AWS AppSyncGraphQL APIs 태그를 지정해야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.

- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.2]AWS Backup복구 지점에 태그를 지정해야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.

- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CloudTrail.7] CloudTrail S3 버킷에서 S3 버킷 액세스 로깅이 활성화되어 있는지 확인합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.1] CodeBuild Bitbucket 소스 리포지토리 URL에는 민감한 보안 인증 정보가 포함되어서는 안 됩니다.
- [CodeBuild.2] CodeBuild 프로젝트 환경 변수에는 클리어 텍스트 보안 인증 정보가 포함되면 안 됩니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다

- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.
- [DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.
- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.

- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.
- [DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.34] EC2 전송 게이트웨이 라우팅 테이블에 태그를 지정해야 합니다.
- [EC2.40] EC2 NAT 게이트웨이에 태그를 지정해야 합니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다
- [EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.
- [EC2.172] EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다

- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.182] Amazon EBS 스냅샷에 대해 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [ECS.18] ECS 작업 정의는 EFS 볼륨에 대해 전송 중 암호화를 사용해야 합니다.
- [ECS.19] ECS 용량 공급자는 관리형 종료 방지 기능이 활성화되어 있어야 합니다.

- [ECS.20] ECS 작업 정의는 Linux 컨테이너 정의에서 루트가 아닌 사용자를 구성해야 합니다.
- [ECS.21] ECS 작업 정의는 Windows 컨테이너 정의에서 관리자가 아닌 사용자를 구성해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다
- [EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.
- [EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.
- [EKS.7] EKS ID 제공업체 구성에 태그를 지정해야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.

- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.3] Elasticsearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [ES.9] Elasticsearch 도메인에 태그를 지정해야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.
- [FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.

- [Glue.1]AWS Glue작업에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.1] GuardDuty를 활성화해야 합니다.
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.
- [GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.7] IAM 사용자를 위한 암호 정책의 구성은 강력해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.10] IAM 사용자의 암호 정책에는 강력한 구성이 있어야 합니다.
- [IAM.11] IAM 암호 정책에서 최소 1개의 대문자를 요구하는지 여부를 확인합니다.
- [IAM.12] IAM 암호 정책에서 최소 1개의 소문자를 요구하는지 여부를 확인합니다.
- [IAM.13] IAM 암호 정책에서 최소 1개의 기호를 요구하는지 여부를 확인합니다.
- [IAM.14] IAM 암호 정책에서 최소 1개의 숫자를 요구하는지 여부를 확인합니다.

- [IAM.15] IAM 암호 정책에서 14자 이상을 요구하는지 여부를 확인합니다.
- [IAM.16] IAM 비밀번호 정책이 비밀번호 재사용을 방지하는지 확인합니다.
- [IAM.17] IAM 암호 정책이 90일 이내에 비밀번호를 만료하도록 하는지 여부를 확인합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoT.4]AWS IoT Core권한 부여자에 태그를 지정해야 합니다.
- [IoT.5]AWS IoT Core역할 별칭에 태그를 지정해야 합니다.
- [IoT.6]AWS IoT Core정책에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.

- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.
- [MQ.4] Amazon MQ 브로커에 태그를 지정해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다

- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.

- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.
- [RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [PCI.Redshift.1] Amazon Redshift 클러스터는 퍼블릭 액세스를 금지해야 합니다.
- [Redshift.2] Amazon Redshift 클러스터에 대한 연결은 전송 중 암호화되어야 합니다.

- [Redshift.3] Amazon Redshift 클러스터에는 자동 스냅샷이 활성화되어 있어야 합니다.
- [Redshift.4] Amazon Redshift 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [Redshift.6] Amazon Redshift에는 메이저 버전으로의 자동 업그레이드가 활성화되어 있어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에 태그를 지정해야 합니다.
- [Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.
- [Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.7] S3 범용 버킷은 리전 간 복제를 사용해야 합니다
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다

- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.
- [S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.

- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.3] Systems Manager가 관리하는 Amazon EC2 인스턴스는 연결 규정 준수 상태가 COMPLIANT여야 합니다.
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## Middle East (Bahrain)

다음 제어는 중동(바레인) 리전에서 지원되지 않습니다.

- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.

- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.10] CloudTrail Lake 이벤트 데이터 스토어는 고객 관리형 로 암호화되어야 합니다.AWS KMS keys
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DocumentDB.6] Amazon DocumentDB 클러스터는 전송 중 암호화되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.20] a AWS Site-to-Site VPN 연결을 위한 두 VPN 터널이 모두 가동되어야 합니다.

- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys
- [ECS.17] ECS 태스크 정의는 호스트 네트워크 모드를 사용해서는 안 됩니다
- [EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.
- [FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.

- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [NetworkFirewall.10] Network Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.41] RDS for SQL Server DB 인스턴스는 전송 중 암호화되어야 합니다.
- [RDS.42] RDS for MariaDB DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.44] RDS for MariaDB DB 인스턴스는 전송 중 암호화되어야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.46] RDS DB 인스턴스를 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다

- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.4] Redshift Serverless 네임스페이스는 고객 관리형으로 암호화해야 합니다.AWS KMS keys
- [RedshiftServerless.5] Redshift Serverless 네임스페이스는 기본 관리자 사용자 이름을 사용해서는 안 됩니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.8] SageMaker 노트북 인스턴스는 지원되는 플랫폼에서 실행되어야 합니다
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 중동(UAE)

다음 제어는 중동(UAE) 리전에서 지원되지 않습니다.

- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFormation.3] CloudFormation 스택에는 종료 방지 기능이 활성화되어 있어야 합니다.
- [CloudFormation.4] CloudFormation 스택에는 연결된 서비스 역할이 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.

- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudTrail.6] CloudTrail 로그를 저장하는 데 사용되는 S3 버킷에 공개적으로 액세스할 수 없는지 확인하세요.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [Detective.1] Detective 동작 그래프에 태그를 지정해야 합니다.
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.3] DMS 이벤트 구독에 태그를 지정해야 합니다.
- [DMS.4] DMS 복제 인스턴스에 태그를 지정해야 합니다.

- [DMS.5] DMS 복제 서브넷 그룹에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.
- [DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.
- [DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.
- [DMS.13] DMS 복제 인스턴스는 여러 가용 영역을 사용하도록 구성되어야 합니다
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.4] 중지된 EC2 인스턴스는 지정된 기간이 지나면 제거해야 합니다.
- [EC2.14] 보안 그룹은 0.0.0.0/0 또는 ::/0에서 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [EC2.180] EC2 네트워크 인터페이스에는 소스/대상 확인이 활성화되어 있어야 합니다
- [EC2.181] EC2 시작 템플릿은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.183] EC2 VPN 연결은 IKEv2 프로토콜을 사용해야 합니다.

- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [EFS.1] Elastic File System은를 사용하여 유휴 파일 데이터를 암호화하도록 구성해야 합니다. AWS KMS
- [EFS.2] Amazon EFS 볼륨은 백업 계획에 포함되어야 합니다.
- [EKS.9] EKS 노드 그룹은 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다
- [ELB.18] Application Load Balancer 및 Network Load Balancer 리스너는 보안 프로토콜을 사용하여 전송 중 데이터를 암호화해야 합니다
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.1] Amazon EMR 클러스터 프라이머리 노드에는 퍼블릭 IP 주소가 없어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.

- [Glue.4]AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue
- [GuardDuty.2] GuardDuty 필터에 태그를 지정해야 합니다.
- [IAM.1] IAM 정책은 전체 "*" 관리 권한을 허용해서는 안 됩니다.
- [IAM.2] IAM 사용자는 IAM 정책을 연결해서는 안 됩니다.
- [IAM.3] IAM 사용자 액세스 키는 90일 이하마다 교체해야 합니다.
- [IAM.4] IAM 루트 사용자 액세스 키가 존재하지 않아야 합니다.
- [IAM.5] 콘솔 암호가 있는 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.8] 사용하지 않은 IAM 사용자 보안 인증을 제거해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.18]를 사용하여 인시던트를 관리하기 위한 지원 역할이 생성되었는지 확인AWS Support
- [IAM.19] 모든 IAM 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.22] 45일 동안 사용하지 않은 IAM 사용자 보안 인증 정보는 제거해야 합니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.
- [Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.
- [Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.

- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [KMS.1] IAM 고객 관리형 정책은 모든 KMS 키에 대한 암호 해독 작업을 허용해서는 안 됩니다.
- [KMS.2] IAM 보안 주체에는 모든 KMS 키에 대한 암호 해독 작업을 허용하는 IAM 인라인 정책이 없어야 합니다.
- [Lambda.7] Lambda 함수에는 AWS X-Ray 활성 추적이 활성화되어 있어야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.4] MSK 클러스터에는 퍼블릭 액세스가 비활성화되어 있어야 합니다
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [MSK.6] MSK 클러스터는 인증되지 않은 액세스를 비활성화해야 합니다
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.

- [Opensearch.9] OpenSearch 도메인에 태그를 지정해야 합니다.
- [Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.
- [Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.18] Redshift 클러스터에는 다중 AZ 배포가 활성화되어 있어야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.

- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SQS.1] Amazon SQS 대기열은 저장 시 암호화되어야 합니다.
- [SQS.2] SQS 대기열에 태그를 지정해야 합니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [SSM.7] SSM 문서에는 퍼블릭 공유 차단 설정이 활성화되어 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## 남아메리카(상파울루)

다음 제어는 남아메리카(상파울루) 리전에서 지원되지 않습니다.

- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다

- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.

- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoT.1]AWS IoT Device Defender보안 프로필에 태그를 지정해야 합니다.
- [IoT.2]AWS IoT Core완화 작업에 태그를 지정해야 합니다.
- [IoT.3]AWS IoT Core차원에 태그를 지정해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다

- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.

## AWS GovCloud (US-East)

AWS GovCloud (US-East) 리전에서는 다음 제어가 지원되지 않습니다.

- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.

- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.
- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.4]AWS AppSyncGraphQL APIs 태그를 지정해야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.

- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.
- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.2] Cognito ID 풀은 인증되지 않은 ID를 허용하면 안 됩니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다

- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다
- [Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.
- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.47] Amazon VPC 엔드포인트 서비스에 태그를 지정해야 합니다.
- [EC2.52] EC2 전송 게이트웨이에 태그를 지정해야 합니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다

- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다
- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.

- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.
- [ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.
- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다

- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [Glue.3]AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.
- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.

- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.
- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.

- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.
- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.31] RDS DB 보안 그룹에 태그를 지정해야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.

- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다
- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.1] Amazon SageMaker 노트북 인스턴스는 인터넷에 직접 액세스할 수 없어야 합니다.
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.16] SageMaker 모델은 기본 컨테이너에 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.19] SageMaker 모델은 다중 컨테이너 추론 파이프라인을 위해 VPC의 프라이빗 레지스트리를 사용해야 합니다.
- [SES.1] SES 연락처 목록에 태그를 지정해야 합니다.
- [SES.2] SES 구성 세트에 태그를 지정해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [SSM.6] SSM Automation에는 CloudWatch 로깅이 활성화되어 있어야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.

- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.
- [WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.
- [WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.

## AWS GovCloud (US-West)

AWS GovCloud (US-West) 리전에서는 다음 제어가 지원되지 않습니다.

- [ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.
- [Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정
- [Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.
- [APIGateway.2] 백엔드 인증을 위해 SSL 인증서를 사용하도록 API Gateway REST API 단계를 구성해야 합니다.
- [APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.
- [APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.
- [APIGateway.10] API Gateway V2 통합은 프라이빗 연결에 HTTPS를 사용해야 합니다.
- [APIGateway.11] API Gateway 도메인 이름은 권장 보안 정책을 사용해야 합니다.
- [Amplify.1] Amplify 앱에 태그를 지정해야 합니다
- [Amplify.2] Amplify 브랜치에 태그를 지정해야 합니다
- [AppConfig.1]AWS AppConfig애플리케이션에 태그를 지정해야 합니다.
- [AppConfig.2]AWS AppConfig구성 프로파일에 태그를 지정해야 합니다.
- [AppConfig.3]AWS AppConfig환경에 태그를 지정해야 합니다.
- [AppConfig.4]AWS AppConfig확장 연결에 태그를 지정해야 합니다.

- [AppFlow.1] Amazon AppFlow 흐름에 태그를 지정해야 합니다
- [AppRunner.1] App Runner 서비스에 태그를 지정해야 합니다
- [AppRunner.2] App Runner VPC 커넥터에 태그를 지정해야 합니다
- [AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.
- [AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.
- [AppSync.4]AWS AppSyncGraphQL APIs 태그를 지정해야 합니다.
- [AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.
- [AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.
- [AutoScaling.2] Amazon EC2 Auto Scaling 그룹은 여러 가용 영역을 포괄해야 합니다.
- [AutoScaling.3] Auto Scaling 그룹 시작 구성은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 요구하도록 EC2 인스턴스를 구성해야 합니다.
- [AutoScaling.6] Auto Scaling 그룹 은 여러 가용 영역에서 여러 인스턴스 유형을 사용해야 합니다.
- [오토스케일링.9] Amazon EC2 Auto Scaling은 Amazon EC2 시작 템플릿을 사용해야 합니다.
- [Backup.4]AWS Backup보고서 계획에 태그를 지정해야 합니다.
- [Batch.1] 배치 작업 대기열에 태그를 지정해야 합니다
- [Batch.2] 배치 예약 정책에 태그를 지정해야 합니다
- [Batch.3] 배치 컴퓨팅 환경에 태그를 지정해야 합니다
- [Batch.4] 관리형 배치 컴퓨팅 환경의 컴퓨팅 리소스 속성에 태그를 지정해야 합니다
- [BedrockAgentCore.1] Bedrock AgentCore 런타임은 VPC 네트워크 모드로 구성해야 합니다.
- [BedrockAgentCore.2] Bedrock AgentCore 게이트웨이는 인바운드 요청에 대한 승인이 필요합니다.
- [BedrockAgentCore.3] Bedrock AgentCore 메모리는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.4] Bedrock AgentCore Gateway는 고객 관리형 AWS KMS키로 암호화해야 합니다.
- [BedrockAgentCore.5] Bedrock AgentCore 사용자 지정 브라우저는 퍼블릭 네트워크 모드를 사용해서는 안 됩니다.
- [BedrockAgentCore.6] Bedrock AgentCore 사용자 지정 브라우저에는 세션 기록이 활성화되어 있어야 합니다.
- [CloudFront.1] CloudFront 배포에는 기본 루트 객체가 구성되어 있어야 합니다.
- [CloudFront.3] CloudFront 배포에는 전송 중 암호화가 필요합니다.

- [CloudFront.4] CloudFront 배포에는 오리진 장애 조치가 구성되어 있어야 합니다.
- [CloudFront.5] CloudFront 배포에는 로깅이 활성화되어 있어야 합니다.
- [CloudFront.6] CloudFront 배포판에는 WAF가 활성화되어 있어야 합니다.
- [CloudFront.7] CloudFront 배포는 사용자 지정 SSL/TLS 인증서를 사용해야 합니다.
- [CloudFront.8] CloudFront 배포는 SNI를 사용하여 HTTPS 요청을 처리해야 합니다.
- [CloudFront.9] CloudFront 배포는 사용자 지정 오리진에 대한 트래픽을 암호화해야 합니다.
- [CloudFront.10] CloudFront 배포는 엣지 로케이션과 사용자 지정 오리진 간에 더 이상 사용되지 않는 SSL 프로토콜을 사용해서는 안 됩니다.
- [CloudFront.12] CloudFront 배포는 존재하지 않는 S3 오리진을 가리키면 안 됩니다.
- [CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.
- [CloudFront.14] CloudFront 배포에 태그를 지정해야 합니다.
- [CloudFront.15] CloudFront 배포는 권장 TLS 보안 정책을 사용해야 합니다
- [CloudFront.16] CloudFront 배포는 Lambda 함수 URL 오리진에 대한 오리진 액세스 제어를 사용해야 합니다
- [CloudFront.17] CloudFront 배포는 서명된 URLs 및 쿠키에 신뢰할 수 있는 키 그룹을 사용해야 합니다.
- [CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.
- [CodeArtifact.1]CodeArtifact 리포지토리에 태그를 지정해야 합니다.
- [CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.
- [CodeBuild.4] CodeBuild 프로젝트 환경에는 로깅 AWS Config요구 사항이 있어야 합니다.
- [CodeGuruProfiler.1] CodeGuru Profiler 프로파일링 그룹에 태그를 지정해야 합니다
- [CodeGuruReviewer.1] CodeGuru Reviewer 리포지토리 연결에 태그를 지정해야 합니다
- [Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다
- [Cognito.3] Cognito 사용자 풀의 암호 정책은 강력한 구성을 사용해야 합니다
- [Cognito.4] Cognito 사용자 풀에는 사용자 지정 인증을 위한 전체 함수 적용 모드로 위협 방지가 활성화되어 있어야 합니다.
- [Cognito.5] Cognito 사용자 풀에 대해 MFA를 활성화해야 합니다.
- [Cognito.6] Cognito 사용자 풀에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Connect.1] Amazon Connect Customer Profiles 객체 유형에 태그를 지정해야 합니다

- [DataSync.2] DataSync 태스크에 태그를 지정해야 합니다
- [DMS.2] DMS 인증서에 태그를 지정해야 합니다.
- [DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.
- [DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.
- [DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.
- [DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.
- [DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.
- [DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.
- [DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [DynamoDB.3] DynamoDB Accelerator(DAX) 클러스터는 저장 시 암호화되어야 합니다.
- [DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다
- [EC2.21] 네트워크 ACL은 0.0.0.0/0에서 포트 22 또는 포트 3389로의 수신을 허용해서는 안 됩니다.
- [EC2.22] 사용하지 않는 Amazon EC2 보안 그룹을 제거해야 합니다.
- [EC2.23] Amazon EC2 Transit Gateway는 VPC 연결 요청을 자동으로 수락하지 않아야 합니다.
- [EC2.24] Amazon EC2 반가상화 인스턴스 유형은 사용할 수 없습니다.
- [EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.
- [EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.
- [EC2.38] EC2 인스턴스에 태그를 지정해야 합니다.
- [EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다
- [EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.
- [EC2.173] 시작 파라미터가 포함된 EC2 스팟 플릿 요청은 연결된 EBS 볼륨에 대한 암호화를 활성화해야 합니다
- [EC2.174] EC2 DHCP 옵션 세트에 태그를 지정해야 합니다
- [EC2.175] EC2 시작 템플릿에 태그를 지정해야 합니다

- [EC2.176] EC2 접두사 목록에 태그를 지정해야 합니다
- [EC2.177] EC2 트래픽 미러 세션에 태그를 지정해야 합니다
- [EC2.178] EC2 트래픽 미러 필터에 태그를 지정해야 합니다
- [EC2.179] EC2 트래픽 미러 대상에 태그를 지정해야 합니다
- [ECR.1] ECR 프라이빗 리포지토리에는 이미지 스캔이 구성되어 있어야 합니다.
- [ECR.2] ECR 프라이빗 리포지토리에는 태그 불변성이 구성되어 있어야 합니다.
- [ECR.3] ECR 리포지토리에는 수명 주기 정책이 하나 이상 구성되어 있어야 합니다.
- [ECR.4] ECR 퍼블릭 리포지토리에 태그를 지정해야 합니다.
- [ECS.3] ECS 작업 정의는 호스트의 프로세스 네임스페이스를 공유해서는 안 됩니다.
- [ECS.4] ECS 컨테이너는 권한이 없는 상태로 실행해야 합니다.
- [ECS.5] ECS 태스크 정의는 루트 파일 시스템에 대한 읽기 전용 액세스로 제한되도록 컨테이너를 구성해야 합니다.
- [ECS.8] 암호는 컨테이너 환경 변수로 전달되어서는 안 됩니다.
- [ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.
- [ECS.10] ECS Fargate 서비스는 최신 Fargate 플랫폼 버전에서 실행되어야 합니다.
- [ECS.12] ECS 클러스터는 Container Insights를 사용해야 합니다.
- [EFS.3] EFS 액세스 포인트는 루트 디렉터리를 적용해야 합니다.
- [EFS.4] EFS 액세스 포인트는 사용자 ID를 적용해야 합니다.
- [EKS.2] EKS 클러스터는 지원되는 Kubernetes 버전에서 실행되어야 합니다.
- [EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.
- [ELB.10] Classic Load Balancer는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.12] Application Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성되어야 합니다.
- [ELB.13] 애플리케이션, 네트워크 및 게이트웨이 로드 밸런서는 여러 가용 영역에 걸쳐 있어야 합니다.
- [ELB.14] Classic Load Balancer는 방어 모드 또는 가장 엄격한 비동기화 완화 모드로 구성해야 합니다.
- [ELB.21] 애플리케이션 및 Network Load Balancer 대상 그룹은 암호화된 상태 확인 프로토콜을 사용해야 합니다.
- [ELB.22] ELB 대상 그룹은 암호화된 전송 프로토콜을 사용해야 합니다.

- [ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다
- [ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.
- [ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.
- [ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.
- [ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.
- [ElastiCache.7] ElastiCache 클러스터는 기본 서브넷 그룹을 사용해서는 안 됩니다.
- [ElasticBeanstalk.1] Elastic Beanstalk 환경에는 향상된 상태 보고 기능이 활성화되어야 합니다.
- [ElasticBeanstalk.2] Elastic Beanstalk 관리형 플랫폼 업데이트가 활성화되어야 합니다.
- [ElasticBeanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.
- [EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.
- [EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다
- [EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다
- [ES.4] CloudWatch Logs에 대한 Elasticsearch 도메인 오류 로깅이 활성화되어야 합니다.
- [EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.
- [EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.
- [FraudDetector.1] Amazon Fraud Detector 엔터티 유형에 태그를 지정해야 합니다
- [FraudDetector.2] Amazon Fraud Detector 레이블에 태그를 지정해야 합니다
- [FraudDetector.3] Amazon Fraud Detector 결과에 태그를 지정해야 합니다
- [FraudDetector.4] Amazon Fraud Detector 변수에 태그를 지정해야 합니다
- [FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.
- [FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.
- [GlobalAccelerator.1] Global Accelerator 액셀러레이터에 태그를 지정해야 합니다.
- [GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.
- [GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.
- [GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.

- [GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다
- [GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다
- [GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다
- [IAM.6]루트 사용자에 대해 하드웨어 MFA를 활성화해야 합니다.
- [IAM.9] 루트 사용자에 대해 MFA를 활성화해야 합니다.
- [IAM.21] 생성한 IAM 고객 관리형 정책은 서비스에 대한 와일드카드 작업을 허용해서는 안 됩니다.
- [IAM.24] IAM 역할에 태그를 지정해야 합니다.
- [IAM.25] IAM 사용자에게 태그를 지정해야 합니다.
- [IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.
- [Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.
- [IoTSiteWise.1]AWSIoT SiteWise 자산 모델에 태그를 지정해야 합니다.
- [IoTSiteWise.2]AWSIoT SiteWise 대시보드에 태그를 지정해야 합니다.
- [IoTSiteWise.3]AWSIoT SiteWise 게이트웨이에 태그를 지정해야 합니다.
- [IoTSiteWise.4]AWSIoT SiteWise 포털에 태그를 지정해야 합니다.
- [IoTSiteWise.5]AWSIoT SiteWise 프로젝트에 태그를 지정해야 합니다.
- [IoTTwinMaker.1]AWSIoT TwinMaker 동기화 작업에 태그를 지정해야 합니다.
- [IoTTwinMaker.2]AWSIoT TwinMaker 워크스페이스에 태그를 지정해야 합니다.
- [IoTTwinMaker.3]AWSIoT TwinMaker 장면에 태그를 지정해야 합니다.
- [IoTTwinMaker.4]AWSIoT TwinMaker 엔터티에 태그를 지정해야 합니다.
- [IoTWireless.1]AWSIoT Wireless 멀티캐스트 그룹에 태그를 지정해야 합니다.
- [IoTWireless.2]AWSIoT Wireless 서비스 프로파일에 태그를 지정해야 합니다.
- [IoTWireless.3]AWSIoT FUOTA 작업에 태그를 지정해야 합니다.
- [IVS.1] IVS 재생 키 페어에 태그를 지정해야 합니다
- [IVS.2] IVS 레코딩 구성에 태그를 지정해야 합니다
- [IVS.3] IVS 채널에 태그를 지정해야 합니다
- [Keyspaces.1] Amazon Keyspaces 키스페이스에 태그를 지정해야 합니다
- [Kinesis.1] Kinesis 스트림은 저장 시 암호화되어야 합니다.
- [KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.
- [Lambda.5] VPC Lambda 함수는 여러 가용 영역에서 작동해야 합니다.

- [Macie.1] Amazon Macie가 활성화되어야 합니다.
- [Macie.2] Macie 민감한 데이터 자동 검색을 활성화해야 합니다.
- [MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.
- [MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다
- [MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.
- [MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.
- [MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.
- [MSK.5] MSK 커넥터에는 로깅이 활성화되어 있어야 합니다
- [Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.
- [Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.
- [Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Neptune.5] Neptune DB 클러스터에는 자동 백업이 활성화되어 있어야 합니다.
- [Neptune.6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.
- [Neptune.7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.
- [Neptune.8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.
- [Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.
- [NetworkFirewall.2] Network Firewall 로깅을 활성화해야 합니다.
- [NetworkFirewall.3] 네트워크 방화벽 정책에는 연결된 규칙 그룹이 하나 이상 있어야 합니다.
- [NetworkFirewall.4] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 전체 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.5] 네트워크 방화벽 정책에 대한 기본 상태 비저장 작업은 조각화된 패킷에 대해 삭제 또는 전달되어야 합니다.
- [NetworkFirewall.6] 상태 비저장 네트워크 방화벽 규칙 그룹은 비어 있으면 안 됩니다.
- [NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.
- [Opensearch.1] OpenSearch 도메인에는 저장 시 암호화가 활성화되어 있어야 합니다.
- [Opensearch.2] OpenSearch 도메인은 공개적으로 액세스할 수 없어야 합니다.
- [Opensearch.3] OpenSearch 도메인은 노드 간에 전송되는 데이터를 암호화해야 합니다.

- [Opensearch.4] CloudWatch Logs에 대한 OpenSearch 도메인 오류 로깅이 활성화되어야 합니다.
- [Opensearch.5] OpenSearch 도메인에는 감사 로깅이 활성화되어 있어야 합니다.
- [Opensearch.6] OpenSearch 도메인에는 데이터 노드가 3개 이상 있어야 합니다.
- [Opensearch.7] OpenSearch 도메인에는 세분화된 액세스 제어가 활성화되어 있어야 합니다.
- [Opensearch.8] OpenSearch 도메인에 대한 연결은 최신 TLS 보안 정책을 사용하여 암호화되어야 합니다.
- [PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.
- [PCA.2]AWS프라이빗 CA 인증 기관에 태그를 지정해야 합니다.
- [RDS.14] Amazon Aurora 클러스터에는 역추적이 활성화되어 있어야 합니다.
- [RDS.15] RDS DB 클러스터는 여러 가용 영역에 대해 구성되어야 합니다.
- [RDS.24] RDS 데이터베이스 클러스터는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.25] RDS 데이터베이스 인스턴스는 사용자 지정 관리자 사용자 이름을 사용해야 합니다.
- [RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.
- [RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.
- [RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- [RDS.43] RDS DB 프록시는 연결에 TLS 암호화를 요구해야 합니다
- [RDS.45] Aurora MySQL DB 클러스터에는 감사 로깅이 활성화되어 있어야 합니다
- [RDS.47] RDS for PostgreSQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.48] RDS for MySQL DB 클러스터는 태그를 DB 스냅샷에 복사하도록 구성되어야 합니다
- [RDS.50] RDS DB 클러스터에는 충분한 백업 보존 기간이 설정되어 있어야 합니다.
- [RDS.51] RDS 글로벌 클러스터는 지원되는 Aurora MySQL 버전에서 실행되어야 합니다.
- [Redshift.7] Redshift 클러스터는 향상된 VPC 라우팅을 사용해야 합니다
- [Redshift.8] Amazon Redshift 클러스터는 기본 관리자 사용자 이름을 사용해서는 안 됩니다.
- [Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다
- [Redshift.11] Redshift 클러스터에 태그를 지정해야 합니다.
- [Redshift.13] Redshift 클러스터 스냅샷에 태그를 지정해야 합니다.
- [Redshift.17] Redshift 클러스터 파라미터 그룹에 태그를 지정해야 합니다
- [RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다

- [RedshiftServerless.2] Redshift Serverless 작업 그룹에 대한 연결은 SSL을 사용하도록 요구해야 합니다
- [RedshiftServerless.3] Redshift Serverless 작업 그룹은 퍼블릭 액세스를 금지해야 합니다
- [RedshiftServerless.6] Redshift Serverless 네임스페이스는 로그를 CloudWatch Logs로 내보내야 합니다
- [Route53.1] Route 53 상태 확인에 태그를 지정해야 합니다.
- [Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.
- [S3.10] 버전 관리가 활성화된 S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.11] S3 범용 버킷에는 이벤트 알림이 활성화되어 있어야 합니다
- [S3.12] S3 범용 버킷에 대한 사용자 액세스를 관리하는 데 ACL을 사용해서는 안 됩니다
- [S3.13] S3 범용 버킷에는 수명 주기 구성이 있어야 합니다
- [S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.
- [S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다
- [S3.25] S3 디렉터리 버킷에는 수명 주기 구성이 있어야 합니다
- [SageMaker.2] SageMaker 노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.
- [SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.
- [SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다
- [SageMaker.6] SageMaker 앱 이미지 구성에 태그를 지정해야 합니다
- [SageMaker.7] SageMaker 이미지에 태그를 지정해야 합니다
- [SageMaker.9] SageMaker 데이터 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.10] SageMaker 모델 설명 가능성 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.11] SageMaker 데이터 품질 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.12] SageMaker 모델 편향 작업 정의에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.13] SageMaker 모델 품질 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.
- [SageMaker.14] SageMaker 모니터링 일정에는 네트워크 격리가 활성화되어 있어야 합니다.
- [SageMaker.15] SageMaker 모델 편향 작업 정의에는 컨테이너 간 트래픽 암호화가 활성화되어 있어야 합니다.

- [SageMaker.17] SageMaker 특성 그룹 오프라인 저장소는 AWS KMS 키로 암호화해야 합니다.
- [SageMaker.18] 표준 스토리지가 있는 SageMaker 특성 그룹 온라인 스토어는 AWS KMS 키로 암호화해야 합니다.
- [SES.3] SES 구성 세트에는 이메일 전송을 위한 TLS가 활성화되어 있어야 합니다.
- [SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.
- [SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다
- [SSM.4] SSM 문서는 공개해서는 안 됩니다.
- [SSM.5] SSM 문서에 태그를 지정해야 합니다
- [StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.
- [StepFunctions.2] Step Functions 활동에는 태그를 지정해야 합니다.
- [Transfer.4] Transfer Family 계약에 태그를 지정해야 합니다
- [Transfer.5] Transfer Family 인증서에 태그를 지정해야 합니다
- [Transfer.6] Transfer Family 커넥터에 태그를 지정해야 합니다
- [Transfer.7] Transfer Family 프로파일에 태그를 지정해야 합니다
- [WAF.1]AWS WAF클래식 글로벌 웹 ACL 로깅을 활성화해야 합니다.
- [WAF.2]AWS WAF클래식 리전 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.3]AWS WAF클래식 리전 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.4]AWS WAF클래식 리전 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.6]AWS WAF클래식 글로벌 규칙에는 하나 이상의 조건이 있어야 합니다.
- [WAF.7]AWS WAF클래식 글로벌 규칙 그룹에는 하나 이상의 규칙이 있어야 합니다.
- [WAF.8]AWS WAF클래식 글로벌 웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.10]AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.
- [WAF.12]AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.

# CloudFormation을 사용하여 Security Hub CSPM 리소스 생성

AWSSecurity Hub CSPMAWS CloudFormation은 리소스 및 인프라를 생성하고 관리하는 데 소요되는 시간을 줄일 수 있도록 AWS리소스를 모델링하고 설정하는 데 도움이 되는 서비스인와 통합됩니다. 원하는 모든 AWS리소스(예: 자동화 규칙)를 설명하는 템플릿을 생성하고 해당 리소스를 CloudFormation프로비저닝하고 구성합니다.

를 사용하면 템플릿을 재사용하여 Security Hub CSPM 리소스를 일관되고 반복적으로 설정할 CloudFormation수 있습니다. 리소스를 한 번 설명한 다음 여러 AWS 계정및 리전에서 동일한 리소스를 반복적으로 프로비저닝합니다.

## Security Hub CSPM 및 CloudFormation템플릿

Security Hub CSPM 및 관련 서비스에 대한 리소스를 프로비저닝하고 구성하려면 CloudFormation 템플릿이 작동하는 방식을 이해해야 합니다. 템플릿은 JSON 또는 YAML 형식의 텍스트 파일입니다. 이러한 템플릿은 CloudFormation스택에서 프로비저닝하려는 리소스를 설명합니다.

JSON 또는 YAML에 익숙하지 않은 경우 CloudFormationDesigner를 사용하여 CloudFormation템플릿을 시작할 수 있습니다. 자세한 내용은 CloudFormationDesigner란 무엇입니까?를 참조하세요. AWS CloudFormation사용 설명서의 .

다음 유형의 Security Hub CSPM 리소스에 대한 CloudFormation템플릿을 생성할 수 있습니다.

- Security Hub CSPM 활성화
- 조직의 위임된 Security Hub CSPM 관리자 지정
- Security Hub CSPM에서 조직이 구성되는 방식을 지정합니다
- 보안 표준 활성화
- 교차 리전 집계 활성화 활성화하기
- 중앙 구성 정책 생성 및 계정, 조직 단위(OU) 또는 루트와 연결
- 사용자 지정 인사이트 생성
- 자동화 규칙 생성
- 제어 파라미터 사용자 지정
- 타사 제품 통합 구독

리소스에 대한 JSON 및 YAML 템플릿의 예제를 비롯한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS Security Hub CSPM 리소스 유형 참조를 참조하세요.

## 에 대해 자세히 알아보기CloudFormation

에 대해 자세히 알아보려면 다음 리소스를 CloudFormation참조하세요.

- AWS CloudFormation
- AWS CloudFormation사용 설명서

- CloudFormationAPI Reference
- AWS CloudFormation명령줄 인터페이스 사용 설명서

# Amazon SNS로 Security Hub CSPM 공지 구독

이 섹션에서는 AWSSecurity Hub CSPM에 대한 알림을 수신하기 위해 Amazon Simple Notification Service(Amazon SNS)를 통해 Security Hub CSPM 공지를 구독하는 방법에 대한 정보를 제공합니다.

구독하면 다음 이벤트에 대한 알림을 받게 됩니다(각 이벤트에 해당하는 `AnnouncementType` 참고).

- `NEW_STANDARDS_CONTROLS` - 새로운 Security Hub CSPM 제어 또는 표준이 추가되었습니다.
- `RETIRED_STANDARDS_CONTROLS` - 기존 Security Hub CSPM 제어 또는 표준이 사용 중지되었습니다.

알림은 Amazon SNS에서 지원하는 모든 형식으로 사용할 수 있습니다. Security Hub CSPM을 사용할 수 있는 모든 AWS 리전에서 Security Hub CSPM 공지를 구독할 수 있습니다.

사용자가 Amazon SNS 주제를 구독할 수 있는 `Subscribe` 권한이 있어야 합니다. Amazon SNS 정책, IAM 정책 또는 둘 다를 사용하여 이를 달성할 수 있습니다. 자세한 정보는 Amazon Simple Notification Service 개발자 안내서에서 IAM 및 Amazon SNS 정책을 함께 참조하세요.

> **Note**
>
> Security Hub CSPM은 구독한 모든 AWS 계정에게 Security Hub CSPM 서비스 업데이트에 대한 Amazon SNS 공지를 전송합니다. Security Hub CSPM 조사 결과에 대한 알림을 받으려면 Security Hub CSPM에서 조사 결과 세부 정보 및 기록 검토 섹션을 참조하세요.

Amazon SNS 주제에 대해 Amazon Simple Queue Service(Amazon SQS) 대기열을 구독할 수 있지만 동일한 리전에 있는 Amazon SNS 주제 Amazon 리소스 이름(ARN)을 사용해야 합니다. 자세한 내용은 Amazon Simple Queue Service 개발자 가이드의 Amazon SNS 주제에 대한 Amazon SQS 대기열 구독을 참조하세요.

알림을 받을 때 AWS Lambda함수를 사용하여 이벤트를 호출할 수도 있습니다. 샘플 함수 코드를 포함한 자세한 내용은 AWS Lambda개발자 안내서의 자습서: Amazon Simple Notification ServiceAWS Lambda에서 사용을 참조하세요.

각 리전에 대한 Amazon SNS 주제 ARN은 다음과 같습니다.

| AWS 리전 | Amazon SNS 주제 ARN |
| --- | --- |
| 미국 동부(오하이오) | arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements |
| 미국 동부(버지니아 북부) | arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements |
| 미국 서부(캘리포니아 북부) | arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements |
| 미국 서부(오리건) | arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements |
| 아프리카(케이프타운) | arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements |
| 아시아 태평양(홍콩) | arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements |
| 아시아 태평양(하이데라바드) | arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements |
| 아시아 태평양(자카르타) | arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements |
| 아시아 태평양(뭄바이) | arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements |

| AWS 리전 | Amazon SNS 주제 ARN |
| --- | --- |
| 아시아 태평양(오사카) | arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements |
| 아시아 태평양(서울) | arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements |
| 아시아 태평양(싱가포르) | arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements |
| 아시아 태평양(시드니) | arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements |
| 아시아 태평양(도쿄) | arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements |
| 캐나다(중부) | arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements |
| 중국(베이징) | arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements |
| 중국(닝샤) | arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements |
| 유럽(프랑크푸르트) | arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements |

| AWS 리전 | Amazon SNS 주제 ARN |
| --- | --- |
| 유럽(아일랜드) | arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements |
| 유럽(런던) | arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements |
| 유럽(밀라노) | arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements |
| 유럽(파리) | arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements |
| 유럽(스페인) | arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements |
| 유럽(스톡홀름) | arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements |
| 유럽(취리히) | arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements |
| 이스라엘(텔아비브) | arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements |
| Middle East (Bahrain) | arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements |

| AWS 리전 | Amazon SNS 주제 ARN |
| --- | --- |
| 중동(UAE) | `arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements` |
| 남아메리카(상파울루) | `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` |

메시지는 일반적으로 파티션 내 여러 리전에서 동일하므로 각 파티션의 한 지역을 구독하면 해당 파티션의 모든 리전에 영향을 미치는 공지를 받을 수 있습니다. 구성원 계정과 관련된 공지는 관리자 계정에 복제되지 않습니다. 따라서 관리자 계정을 포함한 각 계정에는 각 공지사항의 사본이 한 개만 남게 됩니다. Security Hub CSPM 공지를 구독하는 데 사용할 계정을 결정할 수 있습니다.

Security Hub CSPM 공지 구독 비용에 대한 자세한 내용은 Amazon SNS 요금을 참조하세요.

Security Hub CSPM 공지 구독(콘솔)

1. https://console.aws.amazon.com/sns/v3/home에서 Amazon SNS 콘솔을 엽니다.
2. 리전 목록에서 Security Hub CSPM 공지를 구독하려는 리전을 선택합니다. 이 예제에서는 `us-west-2` 리전을 사용합니다.
3. 탐색 창에서 구독을 선택하고 나서 구독 생성을 선택합니다.
4. 주제 ARN 상자에 주제의 ARN을 입력합니다. 예를 들어 `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`입니다.
5. 프로토콜에서 Security Hub CSPM 공지를 수신할 방법을 선택합니다. 이메일을 선택한 경우, 엔드포인트에 공지를 받을 이메일 주소를 입력합니다.
6. 구독 생성을 선택합니다.

7. 구독을 확인합니다. 예를 들어, 이메일 프로토콜을 선택한 경우, Amazon SNS는 사용자가 제공한 이메일로 구독 확인 메시지를 전송합니다.

Security Hub CSPM 공지 구독(AWS CLI)

1. 다음 명령을 실행합니다.

```
 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. 구독을 확인합니다. 예를 들어, 이메일 프로토콜을 선택한 경우, Amazon SNS는 사용자가 제공한 이메일로 구독 확인 메시지를 전송합니다.

## Amazon SNS 메시지 형식

다음 예제는 Amazon SNS에서 전송한 새로운 보안 제어 도입에 대한 Security Hub CSPM 공지를 보여줍니다. 메시지 내용은 공지 유형에 따라 다르지만 형식은 모든 공지 유형에서 동일합니다. 선택적으로 공지 사항에 대한 세부 정보를 제공하는 `Link` 필드가 포함될 수 있습니다.

예제: 새로운 제어에 대한 Security Hub CSPM 공지(이메일 프로토콜)

```
{
"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. "
}
```

예제: 새로운 제어에 대한 Security Hub CSPM 공지(이메일-JSON 프로토콜)

```
{
  "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"
}
```

# Security Hub CSPM 비활성화

AWSSecurity Hub CSPM 콘솔 또는 Security Hub API를 사용하여 Security Hub CSPM을 비활성화할 수 있습니다. Security Hub CSPM을 비활성화한 경우 나중에 다시 활성화할 수 있습니다.

조직에서 중앙 구성을 사용하는 경우, 위임된 Security Hub CSPM 관리자는 특정 계정 및 조직 단위(OU)에서 Security Hub CSPM을 비활성화하고 다른 계정 및 OU에서는 Security Hub CSPM를 활성화하도록 유지하는 구성 정책을 생성할 수 있습니다. 구성 정책은 홈 리전 및 연결된 모든 리전에 영향을 미칩니다. 자세한 내용은 Security Hub CSPM의 중앙 구성 이해 단원을 참조하십시오.

계정에서 Security Hub CSPM을 비활성화하면 다음과 같은 결과가 발생합니다.

- 계정에서 모든 Security Hub CSPM 표준 및 제어가 비활성화됩니다.
- Security Hub CSPM이 계정에 대한 조사 결과 생성, 업데이트 및 수집을 중지합니다.
- 30일 후 Security Hub CSPM이 계정의 모든 기존 보관된 조사 결과를 영구적으로 삭제합니다. Security Hub CSPM을 사용하여 조사 결과를 복구할 수 없습니다.
- 90일 후 Security Hub CSPM이 계정의 모든 기존 활성 조사 결과를 영구적으로 삭제합니다. Security Hub CSPM을 사용하여 조사 결과를 복구할 수 없습니다.
- 90일 후 Security Hub CSPM이 계정의 모든 기존 인사이트 및 Security Hub CSPM 구성 설정을 영구적으로 삭제합니다. 데이터 및 설정을 복구할 수 없습니다.

기존 조사 결과를 유지하려면 Security Hub CSPM을 비활성화하기 전에 조사 결과를 S3 버킷으로 내보낼 수 있습니다. 이 작업은 Amazon EventBridge 규칙과 함께 사용자 지정 작업을 사용하여 수행할 수 있습니다. 자세한 내용은 자동 응답 및 문제 해결을 위해 EventBridge 사용 단원을 참조하십시오.

계정에서 Security Hub CSPM을 비활성화한 후 90일 이내에 다시 활성화하는 경우, 기존 활성 조사 결과와 계정에 대한 인사이트 및 Security Hub CSPM 구성 설정에 다시 액세스할 수 있습니다. 30일 이내에 Security Hub CSPM을 다시 활성화하는 경우 계정의 기존 보관된 조사 결과에도 다시 액세스할 수 있습니다. 그러나 Security Hub CSPM을 비활성화하면 AWS환경 상태가 반영되므로 기존 결과가 정확하지 않을 수 있습니다. 또한 개별 표준 및 제어를 다시 활성화하면 Security Hub CSPM은 처음에 활성화하는 표준 및 제어에 따라 특정 AWS리소스에 대해 중복 조사 결과를 생성할 수 있습니다. 이러한 이유로 다음 중 하나를 수행하는 것이 좋습니다.

- Security Hub CSPM을 비활성화하기 전에 모든 기존 조사 결과의 워크플로 상태를 `RESOLVED`로 변경합니다. 자세한 내용은 조사 결과에 대한 워크플로 상태 설정 단원을 참조하십시오.

- Security Hub CSPM을 비활성화하기 최소 6일 전에 모든 표준을 비활성화합니다. 그러면 Security Hub CSPM은 일반적으로 3~5일 이내에 모든 기존 조사 결과를 최대한 보관합니다. 자세한 내용은 표준 비활성화 단원을 참조하십시오.

다음과 같은 경우에는 Security Hub CSPM을 비활성화할 수 없습니다.

- 계정이 조직의 위임된 Security Hub CSPM 관리자 계정입니다. 중앙 구성을 사용하는 경우, 위임된 관리자 계정에 Security Hub CSPM을 비활성화하는 구성 정책을 연결할 수 없습니다. 다른 계정에는 연결할 수 있지만 Security Hub CSPM은 해당 정책을 위임된 관리자 계정에 적용하지 않습니다.
- 계정이 초대에 의한 Security Hub CSPM 관리자 계정이며 멤버 계정이 있습니다. Security Hub CSPM을 비활성화하려면 먼저 모든 멤버 계정을 연결 해제해야 합니다. 자세한 방법은 the section called “멤버 계정 연결 해제”을 참조하세요.

멤버 계정에서 Security Hub CSPM을 비활성화하려면 먼저 계정을 관리자 계정에서 연결 해제해야 합니다. 조직 계정의 경우, 관리자 계정만 멤버 계정을 연결 해제할 수 있습니다. 자세한 내용은 the section called “조직 멤버 계정의 연결 해제” 단원을 참조하십시오. 수동으로 초대된 계정의 경우, 관리자 계정 또는 멤버 계정이 계정을 연결 해제할 수 있습니다. 자세한 내용은 the section called “멤버 계정 연결 해제” 또는 the section called “관리자 계정에서 연결 해제”을 참조하세요. 중앙 구성을 사용하는 경우, Security Hub CSPM 관리자가 특정 멤버 계정에서 Security Hub CSPM을 비활성화하는 정책을 만들 수 있으므로 연결 해제가 필요하지 않습니다.

계정에 대해 Security Hub CSPM을 비활성화하면 현재 에서만 비활성화됩니다AWS 리전. 하지만 중앙 구성을 사용하여 특정 계정에서 Security Hub CSPM을 비활성화하면 홈 리전 및 연결된 모든 리전에서 Security Hub CSPM이 비활성화됩니다.

Security Hub CSPM을 비활성화하려면 원하는 방법을 선택하고 단계를 수행합니다.

Security Hub CSPM console

콘솔을 사용하여 Security Hub CSPM을 비활성화하려면 다음 단계를 따르세요.

Security Hub CSPM을 비활성화하려면

1. https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. Security Hub CSPM 비활성화 섹션에서 Security Hub CSPM 비활성화를 선택합니다.
4. 확인 메시지가 나타나면 Security Hub CSPM 비활성화를 선택합니다.

Security Hub API

프로그래밍 방식으로 Security Hub CSPM을 비활성화하려면 AWSSecurity Hub API의 DisableSecurityHub 작업을 사용합니다. 또는를 사용하는 경우 disable-security-hub 명령을 AWS CLI실행합니다. 예를 들어 다음 명령은 현재에서 Security Hub CSPM을 비활성화합니다.AWS 리전

```
$ aws securityhub disable-security-hub
```

# 의 보안 AWS Security Hub CSPM

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 클라우드에서 AWS AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사원은 정기적으로 AWS 규제 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS Security Hub CSPM에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내의AWS 서비스를 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Security Hub CSPM을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 Security Hub CSPM을 구성하는 방법을 보여줍니다. 또한 Security Hub CSPM 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- 의 데이터 보호 AWS Security Hub CSPM
- AWS Security Hub CSPM의 Identity and Access Management
- 에 대한 규정 준수 검증 AWS Security Hub CSPM
- AWS Security Hub의 복원력

- 의 인프라 보안 AWS Security Hub CSPM
- AWS Security Hub CSPM 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

## 의 데이터 보호 AWS Security Hub CSPM

AWS 공동 책임 모델 은 AWS Security Hub CSPM의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 일반 데이터 보호 규정(GDPR) 센터를 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Security Hub CSPM 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

Security Hub CSPM은 멀티테넌트 서비스입니다. 데이터 보호를 보장하기 위해 Security Hub CSPM은 저장된 데이터와 구성 요소 서비스 간에 전송 중인 데이터를 암호화합니다.

# AWS Security Hub CSPM의 Identity and Access Management

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 어떤 사용자가 Security Hub 리소스를 사용하도록 인증(로그인) 및 권한 부여(권한 소유)될 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제


- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- IAM에서 Security Hub의 작동 방식
- 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM
- 에 대한 서비스 연결 역할 AWS Security Hub CSPM
- AWS Security Hub에 대한 관리형 정책
- AWS Security Hub CSPM 자격 증명 및 액세스 문제 해결


## 대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조AWS Security Hub CSPM 자격 증명 및 액세스 문제 해결)
- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(IAM에서 Security Hub의 작동 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 참조)

## ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

## 정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

### ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

### 리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

### 기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

### 여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

## IAM에서 Security Hub의 작동 방식

AWS Identity and Access Management (IAM)를 사용하여 액세스를 관리하기 전에 Security Hub CSPM에서 사용할 수 있는 IAM 기능을 AWS Security Hub CSPM알아봅니다.

에서 사용할 수 있는 IAM 기능 AWS Security Hub CSPM

| IAM 특성 | Security Hub CSPM 지원 |
|---|---|
| 자격 증명 기반 정책 | 예 |
| 리소스 기반 정책 | 아니요 |
| 정책 작업 | 예 |
| 정책 리소스 | 아니요 |
| 정책 조건 키 | 예 |
| 액세스 제어 목록(ACL) | 아니요 |

| IAM 특성 | Security Hub CSPM 지원 |
| --- | --- |
| ABAC(속성 기반 액세스 제어) - 정책 태그 | 예 |
| 임시 보안 인증 | 예 |
| 전달 액세스 세션(FAS) | 예 |
| 서비스 역할 | 아니요 |
| 서비스 연결 역할 | 예 |

Security Hub CSPM 및 기타에서 대부분의 IAM 기능을 AWS 서비스 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS 서비스 IAM으로 작업하는 섹션을 참조하세요.

Security Hub CSPM에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Security Hub CSPM은 자격 증명 기반 정책을 지원합니다. 자세한 내용은 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 단원을 참조하십시오.

Security Hub CSPM에 대한 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

Security Hub CSPM은 리소스 기반 정책을 지원하지 않습니다. Security Hub CSPM 리소스에는 IAM 정책을 직접 연결할 수 없습니다.

Security Hub CSPM에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Security Hub CSPM의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
securityhub:
```

예를 들어 Security Hub CSPM API의 `EnableSecurityHub` 작업에 해당하는 작업인 Security Hub CSPM을 활성화할 수 있는 권한을 사용자에게 부여하려면 해당 `securityhub:EnableSecurityHub` 정책을 포함합니다. 정책 문에는 `Action` 또는 `NotAction` 요소가 포함되어야 합니다. Security Hub CSPM은이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

```
"Action": "securityhub:EnableSecurityHub"
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다. 예제:

```
"Action": [
      "securityhub:EnableSecurityHub",
      "securityhub:BatchEnableStandards"
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수도 있습니다. 예를 들어, `Get`라는 단어로 시작하는 모든 작업을 지정하려면 다음 작업을 포함합니다.

```
"Action": "securityhub:Get*"
```

하지만 가장 좋은 방법은 최소 권한의 원칙을 따르는 정책을 만드는 것입니다. 즉, 특정 작업을 수행하는 데 필요한 권한만 포함하는 정책을 만들어야 합니다.

`BatchGetSecurityControls`, `BatchGetStandardsControlAssociations` 및 `ListStandardsControlAssociations`에 액세스하려면 사용자가 `DescribeStandardsControl` 작업에 액세스할 수 있어야 합니다.

`BatchUpdateStandardsControlAssociations` 및 `UpdateSecurityControl`에 액세스하려면 사용자가 `UpdateStandardsControls` 작업에 액세스할 수 있어야 합니다.

Security Hub CSPM 작업 목록은 서비스 승인 참조의에서 정의한 작업을 AWS Security Hub CSPM 참조하세요. Security Hub CSPM 작업을 지정하는 정책의 예는 섹션을 참조하세요에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM.

Security Hub CSPM에 대한 정책 리소스

정책 리소스 지원: 아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Security Hub CSPM은 다음과 같은 리소스 유형을 정의합니다.

- Hub(허브)
- 제품
- 교차 리전 집계자라고도 하는 조사 결과 집계자
- 자동화 규칙
- 구성 정책

ARN을 사용하여 정책에서 이러한 유형의 리소스를 지정할 수 있습니다.

Security Hub CSPM 리소스 유형 및 각 리소스의 ARN 구문 목록은 서비스 승인 참조의에서 정의한 리소스 유형을 AWS Security Hub CSPM 참조하세요. 각 리소스 유형으로 지정할 수 있는 작업을 알아보

려면 서비스 승인 참조의 AWS Security Hub CSPM에서 정의한 작업 섹션을 참조하세요. 리소스를 지정하는 정책의 예제는 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 섹션을 참조하세요.

Security Hub CSPM에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Security Hub CSPM 조건 키 목록은 서비스 권한 부여 참조의에 대한 조건 키를 AWS Security Hub CSPM 참조하세요. 조건 키와 함께 사용할 수 있는 작업 및 리소스를 알아보려면 AWS Security Hub CSPM에서 정의한 작업을 참조하세요. 조건 키를 사용하는 정책의 예제는 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM을 참조하세요.

Security Hub CSPM의 액세스 제어 목록(ACLs)

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Security Hub CSPM은 ACLs 지원하지 않으므로 Security Hub CSPM 리소스에 ACL을 연결할 수 없습니다.

Security Hub CSPM을 사용한 ABAC(속성 기반 액세스 제어)

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Security Hub CSPM 리소스에 태그를 연결할 수 있습니다. 또한 정책 `Condition` 요소에 태그 정보를 제공하여 리소스에 대한 액세스를 제어할 수도 있습니다.

Security Hub CSPM 리소스 태그 지정에 대한 자세한 내용은 섹션을 참조하세요Security Hub 리소스 태그 지정. 태그를 기반으로 리소스에 대한 액세스를 제한하는 ID 기반 정책의 예제는 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM 섹션을 참조하세요.

Security Hub CSPM에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용자 설명서의 IAM 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

임시 보안 인증을 사용하여 페더레이션을 통해 로그인하거나, IAM 역할을 맡거나, 교차 계정 역할을 맡을 수 있습니다. AssumeRole 또는 GetFederationToken과 같은 AWS STS API 작업을 호출하여 임시 보안 자격 증명을 얻습니다.

Security Hub CSPM은 임시 자격 증명 사용을 지원합니다.

Security Hub CSPM에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

예를 들어 Security Hub CSPM은 Security Hub CSPM을와 AWS 서비스 통합 AWS Organizations 하고 Organizations에서 조직의 위임된 Security Hub CSPM 관리자 계정을 지정할 때 다운스트림에 FAS 요청을 보냅니다.

다른 작업의 경우 Security Hub CSPM은 서비스 연결 역할을 사용하여 사용자를 대신하여 작업을 수행합니다. 이 역할에 대한 자세한 내용은 에 대한 서비스 연결 역할 AWS Security Hub CSPM 섹션을 참조하세요.

Security Hub CSPM의 서비스 역할

Security Hub CSPM은 서비스 역할을 수임하거나 사용하지 않습니다. 사용자를 대신하여 작업을 수행하기 위해 Security Hub CSPM은 서비스 연결 역할을 사용합니다. 이 역할에 대한 자세한 내용은 에 대한 서비스 연결 역할 AWS Security Hub CSPM 섹션을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Security Hub CSPM 사용 시 운영 문제가 발생할 수 있습니다. Security Hub CSPM이 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Security Hub CSPM에 대한 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 태스크를 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Security Hub CSPM은 서비스 연결 역할을 사용하여 사용자를 대신하여 작업을 수행합니다. 이 역할에 대한 자세한 내용은 에 대한 서비스 연결 역할 AWS Security Hub CSPM 섹션을 참조하세요.

## 에 대한 자격 증명 기반 정책 예제 AWS Security Hub CSPM

기본적으로 사용자 및 역할은 Security Hub CSPM 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console AWS CLI또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 관리자는 지정된 리소스에서 특정 API 태스크를 수행할 수 있는 권한을 사용자와 역할에게 부여하는 IAM 정책을 생성해야 합니다. 그런 다음 관리자는 해당 권한이 필요한 사용자 또는 그룹에 이러한 정책을 연결해야 합니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용자 설명서의 JSON 탭에서 정책 생성을 참조하세요.

주제

- 정책 모범 사례
- Security Hub CSPM 콘솔 사용
- 예제: 사용자가 자신이 권한을 볼 수 있도록 허용
- 예제: 사용자가 구성 정책을 생성하고 관리하도록 허용
- 예제: 사용자가 조사 결과를 볼 수 있도록 허용

- 예제: 사용자가 자동화 규칙을 생성하고 관리하도록 허용

### 정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Security Hub 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

### Security Hub CSPM 콘솔 사용

AWS Security Hub CSPM 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 Security Hub CSPM 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정.

최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

이러한 사용자와 역할이 Security Hub CSPM 콘솔을 사용할 수 있도록 하려면 다음 AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용자 설명서의 사용자에게 권한 추가를 참조하세요.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

예제: 사용자가 자신이 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여 줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "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": "*"
        }
    ]
}
```

예제: 사용자가 구성 정책을 생성하고 관리하도록 허용

이 예제에서는 사용자가 구성 정책을 생성, 보기, 업데이트 및 삭제할 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다. 또한 이 예제 정책을 통해 사용자는 정책 연결을 시작, 중지 및 볼 수 있습니다. 이 IAM 정책이 작동하려면 사용자가 조직의 위임된 Security Hub CSPM 관리자여야 합니다.

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": "*"
        }
```

```
    ]
}
```

예제: 사용자가 조사 결과를 볼 수 있도록 허용

이 예제에서는 사용자가 Security Hub CSPM 결과를 볼 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewFindings",
            "Effect": "Allow",
            "Action": [
                "securityhub:GetFindings"
            ],
            "Resource": "*"
        }
    ]
}
```

예제: 사용자가 자동화 규칙을 생성하고 관리하도록 허용

이 예제에서는 사용자가 Security Hub CSPM 자동화 규칙을 생성, 보기, 업데이트 및 삭제할 수 있도록 허용하는 IAM 정책을 생성하는 방법을 보여줍니다. 이 IAM 정책이 작동하려면 사용자가 Security Hub CSPM 관리자여야 합니다. 예를 들어, 사용자가 자동화 규칙만 볼 수 있도록 권한을 허용하려면 생성, 업데이트 및 삭제 권한을 제거할 수 있습니다.

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": "*"
        }
    ]
}
```

## 에 대한 서비스 연결 역할 AWS Security Hub CSPM

AWS Security Hub CSPM 는 라는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다`AWSServiceRoleForSecurityHub`. 이 서비스 연결 역할은 Security Hub CSPM에 직접 연결된 IAM 역할입니다. Security Hub CSPM에서 사전 정의하며, Security Hub CSPM이 사용자를 대신하여 다른를 호출 AWS 서비스 하고 AWS 리소스를 모니터링하는 데 필요한 모든 권한을 포함합니다. Security Hub CSPM은 Security Hub CSPM을 사용할 수 AWS 리전 있는 모든에서이 서비스 연결 역할을 사용합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Security Hub CSPM을 더 쉽게 설정할 수 있습니다. Security Hub CSPM은 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않은 한 Security Hub CSPM만 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 개체에 연결할 수 없습니다.

Security Hub CSPM 콘솔을 사용하여 서비스 연결 역할의 세부 정보를 검토할 수 있습니다. 탐색 창의 설정 아래에서 일반을 선택합니다. 그런 다음 서비스 권한 섹션에서 서비스 권한 보기를 선택합니다.

Security Hub CSPM이 활성화된 모든 리전에서 Security Hub CSPM을 비활성화한 후에만 Security Hub CSPM 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 액세스 권한을 실수로 제거할 수 없기 때문에 Security Hub CSPM 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM 사용자 설명서에서 IAM으로 작업하는AWS 서비스를 살펴보고 서비스 연결 역할 열이 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

주제


- Security Hub CSPM에 대한 서비스 연결 역할 권한
- Security Hub CSPM에 대한 서비스 연결 역할 생성
- Security Hub CSPM에 대한 서비스 연결 역할 편집
- Security Hub CSPM에 대한 서비스 연결 역할 삭제


## Security Hub CSPM에 대한 서비스 연결 역할 권한

Security Hub CSPM은 라는 서비스 연결 역할을 사용합니다`AWSServiceRoleForSecurityHub`. 가 리소스에 액세스하는 AWS Security Hub CSPM 데 필요한 서비스 연결 역할입니다. 이 서비스 연결 역할을 통해 Security Hub CSPM은 다른 로부터 조사 결과를 수신 AWS 서비스 하고 제어에 대한 보안 검사를 실행하는 데 필요한 AWS Config 인프라를 구성하는 등의 작업을 수행할 수 있습니다. `AWSServiceRoleForSecurityHub` 서비스 연결 역할은 역할을 수임하기 위해 `securityhub.amazonaws.com`서비스를 신뢰합니다.

`AWSServiceRoleForSecurityHub` 서비스 연결 역할은 관리형 정책 `AWSSecurityHubServiceRolePolicy`을(를) 사용합니다.

IAM ID(역할, 그룹, 사용자 등)가 서비스 연결 역할을 작성하고 편집하거나 삭제할 수 있도록 권한을 부여해야 합니다. `AWSServiceRoleForSecurityHub` 서비스 연결 역할을 성공적으로 생성하려면 Security Hub CSPM에 액세스하는 데 사용하는 IAM 자격 증명에 필요한 권한이 있어야 합니다. 필수 권한을 부여하려면 다음 정책을 IAM ID에 연결하세요.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "securityhub.amazonaws.com"
                }
            }
        }
    ]
}
```

### Security Hub CSPM에 대한 서비스 연결 역할 생성

Security Hub CSPM을 처음 활성화하거나 이전에 활성화하지 않은 리전에서 Security Hub CSPM을 활성화하면 `AWSServiceRoleForSecurityHub` 서비스 연결 역할이 자동으로 생성됩니다. 또한 IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 `AWSServiceRoleForSecurityHub` 서비스 연결 역할을 수동으로 생성할 수 있습니다. 수동 서비스 역할 생성에 대한 자세한 내용은 IAM 사용자 설명서의 서비스에 대한 역할 만들기를 참조하세요.

> **Important**
>
> Security Hub CSPM 관리자 계정에 대해 생성된 서비스 연결 역할은 연결된 Security Hub CSPM 멤버 계정에 적용되지 않습니다.

### Security Hub CSPM에 대한 서비스 연결 역할 편집

Security Hub CSPM에서는 `AWSServiceRoleForSecurityHub` 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 그러나 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

### Security Hub CSPM에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔티티가 없도록 합니다.

Security Hub CSPM을 비활성화해도 Security Hub CSPM은 `AWSServiceRoleForSecurityHub` 서비스 연결 역할을 자동으로 삭제하지 않습니다. Security Hub CSPM을 다시 활성화하면 서비스가 기존 서비스 연결 역할을 다시 사용하기 시작할 수 있습니다. Security Hub CSPM을 더 이상 사용할 필요가 없는 경우 서비스 연결 역할을 수동으로 삭제할 수 있습니다.

> **Important**
>
> `AWSServiceRoleForSecurityHub` 서비스 연결 역할을 삭제하기 전에 먼저 서비스 연결 역할이 활성화된 모든 리전에서 Security Hub CSPM을 비활성화해야 합니다. 자세한 내용은 Security Hub CSPM 비활성화 단원을 참조하십시오. 서비스 연결 역할을 삭제하려고 할 때 Security Hub CSPM이 비활성화되지 않으면 삭제가 실패합니다.

`AWSServiceRoleForSecurityHub` 서비스 연결 역할을 삭제하려면 IAM 콘솔, IAM CLI 또는 IAM API를 사용할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

## AWS Security Hub에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 줍니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 될 때 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용자 가이드의 AWS 관리형 정책을 참조하세요.

### AWS 관리형 정책: AWSSecurityHubFullAccess

`AWSSecurityHubFullAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 모든 Security Hub CSPM 작업에 대한 전체 액세스 권한을 허용하는 관리 권한을 위탁자에게 부여합니다. 위탁자가 자신의 계정에 대해 Security Hub CSPM을 수동으로 활성화하려면 먼저 위탁자에 이 정책을 연결해야 합니다. 예를 들어, 이러한 권한이 있는 보안 주체는 조사 결과의 상태를 보고 업데이트할 수 있습니다. 또한 사용자 지정 인사이트를 구성하고, 통합을 활성화하고, 표준 및 제어를 활성화/비활성화할 수 있습니다. 관리자 계정의 보안 주체는 멤버 계정을 관리할 수도 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `securityhub` – 위탁자가 Security Hub CSPM 작업에 대한 전체 액세스 권한을 가질 수 있습니다.
- `guardduty` - 보안 주체가 Amazon GuardDuty에서 탐지기, 조직 관리자 관리, 멤버 계정 관리 및 조직 전체 구성에 대한 전체 수명 주기 관리를 수행할 수 있습니다. 여기에는 GetDetector, ListDetector, CreateDetector, UpdateDetector, DeleteDetector, EnableOrganizationAdminAccount, ListOrganizationAdminAccounts, CreateMembers, UpdateOrganizationConfiguration, DescribeOrganizationConfiguration 등의 API 작업이 포함됩니다.
- `iam` - 보안 주체가 Security Hub CSPM 및 Security Hub에 대한 서비스 연결 역할을 생성하고 역할, 정책 및 정책 버전을 가져올 수 있도록 허용합니다.
- `inspector` - 보안 주체가 계정 상태에 대한 정보를 가져오고, 활성화 또는 비활성화하고, 관리자 관리를 위임하고, Amazon Inspector에서 조직 구성 관리를 수행할 수 있습니다. 여기에는 BatchGetAccountStatus, 활성화, 비활성화, EnableDelegatedAdminAccount, DisableDelegatedAdminAccount, ListDelegatedAdminAccounts, UpdateOrganizationConfiguration, DescribeOrganizationConfiguration 등의 API 작업이 포함됩니다.
- `pricing` - 보안 주체가 AWS 서비스 및 제품의 가격 목록을 가져올 수 있도록 허용합니다.
- `account` - 보안 주체가 Security Hub에서 리전 관리를 지원하기 위해 계정 리전에 대한 정보를 가져올 수 있도록 허용합니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubFullAccess를 참조하세요.

AWS 관리형 정책: AWSSecurityHubReadOnlyAccess

`AWSSecurityHubReadOnlyAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 Security Hub CSPM의 정보를 볼 수 있는 읽기 전용 권한을 사용자에게 부여합니다. 이 정책이 연결된 위탁자는 Security Hub CSPM에서 업데이트를 수행할 수 없습니다. 예를 들어, 이러한 권한이 있는 보안 주체는 자신의 계정과 연결된 조사 결과 목록을 볼 수 있지만 조사 결과의 상태를 변경할

수는 없습니다. 이들은 인사이트 결과는 볼 수 있지만 사용자 지정 인사이트를 만들거나 구성할 수는 없습니다. 이들은 제어 기능 또는 제품 통합을 구성할 수 없습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `securityhub` - 사용자가 항목 목록 또는 특정 항목의 세부 정보를 반환하는 작업을 수행할 수 있습니다. 여기에는 `Get`, `List` 또는 `Describe`(으)로 시작하는 API 작업이 포함됩니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubReadOnlyAccess를 참조하세요.

AWS 관리형 정책: AWSSecurityHubOrganizationsAccess

`AWSSecurityHubOrganizationsAccess` 정책을 IAM ID에 연결할 수 있습니다.

이 정책은 조직에 대해 Security Hub, Security Hub CSPM, Amazon GuardDuty 및 Amazon Inspector를 활성화하고 관리할 수 있는 관리 권한을 부여합니다 AWS Organizations. 이 정책에 대한 권한을 통해 조직 관리 계정은 Security Hub, Security Hub CSPM, Amazon GuardDuty 및 Amazon Inspector에 대한 위임된 관리자 계정을 지정할 수 있습니다. 또한, 위임된 관리자 계정을 통해 조직 계정을 멤버 계정으로 활성화할 수 있습니다.

이 정책은에 대한 권한만 제공합니다 AWS Organizations. 조직 관리 계정 및 위임된 관리자 계정에도 관련 작업에 대한 권한이 필요합니다. `AWSSecurityHubFullAccess` 관리형 정책을 사용하여 이러한 권한을 부여할 수 있습니다.

관리 계정에서 위임된 관리자 정책을 생성하거나 업데이트하려면이 정책에 제공되지 않은 추가 권한이 필요합니다. 이러한 작업을 수행하려면 AWSOrganizationsFullAccess 정책에 대한 권한을 추가`organizations:PutResourcePolicy`하거나 연결하는 것이 좋습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `organizations:ListAccounts` – 보안 주체가 조직의 일부인 계정 목록을 검색할 수 있습니다.
- `organizations:DescribeOrganization` – 보안 주체가 조직에 대한 정보를 검색할 수 있습니다.
- `organizations:ListRoots` – 보안 주체가 조직의 루트를 나열할 수 있습니다.

- organizations:ListDelegatedAdministrators - 보안 주체가 조직의 위임된 관리자를 나열할 수 있습니다.
- organizations:ListAWSServiceAccessForOrganization - 보안 주체 AWS 서비스 가 조직에서 사용하는를 나열할 수 있도록 허용합니다.
- organizations:ListOrganizationalUnitsForParent – 보안 주체가 상위 OU의 하위 조직 단위(OU)를 나열할 수 있습니다.
- organizations:ListAccountsForParent – 보안 주체가 상위 OU의 하위 계정을 나열할 수 있습니다.
- organizations:ListParents - 지정된 하위 조직 단위(OU) 또는 계정의 직속 상위 역할을 하는 루트 또는 OU를 나열합니다.
- organizations:DescribeAccount – 보안 주체가 조직의 계정에 대한 정보를 검색할 수 있습니다.
- organizations:DescribeOrganizationalUnit – 보안 주체가 조직의 OU에 대한 정보를 검색할 수 있습니다.
- organizations:ListPolicies - 지정된 유형의 조직에 있는 모든 정책의 목록을 검색합니다.
- organizations:ListPoliciesForTarget - 지정된 대상 루트, 조직 단위(OU) 또는 계정에 직접 연결된 정책을 나열합니다.
- organizations:ListTargetsForPolicy - 지정된 정책이 연결된 모든 루트, 조직 단위(OU) 및 계정을 나열합니다.
- organizations:EnableAWSServiceAccess – 위탁자가 Organizations를 통합할 수 있도록 허용합니다.
- organizations:RegisterDelegatedAdministrator – 위탁자가 위임된 관리자 계정을 지정할 수 있도록 허용합니다.
- organizations:DeregisterDelegatedAdministrator – 위탁자가 위임된 관리자 계정을 제거할 수 있도록 허용합니다.
- organizations:DescribePolicy - 정책에 대한 정보를 검색합니다.
- organizations:DescribeEffectivePolicy - 지정된 정책 유형 및 계정에 대한 유효 정책의 내용을 반환합니다.
- organizations:CreatePolicy - 루트, 조직 단위(OU) 또는 개별 AWS 계정에 연결할 수 있는 지정된 유형의 정책을 생성합니다.
- organizations:UpdatePolicy - 기존의 정책을 새로운 이름, 설명 또는 내용으로 업데이트합니다.
- organizations:DeletePolicy - 조직에서 지정된 정책을 삭제합니다.

- `organizations:AttachPolicy` - 정책을 루트, 조직 단위(OU) 또는 개인 계정에 연결합니다.
- `organizations:DetachPolicy` - 대상 루트, 조직 단위(OU) 또는 계정에서 정책을 분리합니다.
- `organizations:EnablePolicyType` - 루트에서 정책 유형을 활성화합니다.
- `organizations:DisablePolicyType` - 루트에서 조직 정책 유형을 비활성화합니다.
- `organizations:TagResource` - 지정된 리소스에 하나 이상의 태그를 추가합니다.
- `organizations:UntagResource` - 지정된 리소스에서 지정된 키가 있는 태그를 모두 제거합니다.
- `organizations:ListTagsForResource` - 지정된 리소스에 연결된 태그를 나열합니다.
- `organizations:DescribeResourcePolicy` - 리소스 정책에 대한 정보를 검색합니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubOrganizationsAccess를 참조하세요.

AWS 관리형 정책: AWSSecurityHubServiceRolePolicy

`AWSSecurityHubServiceRolePolicy`를 IAM 엔티티에 연결할 수 없습니다. 이 정책은 Security Hub CSPM에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결되어 있습니다. 자세한 내용은 the section called “서비스 연결 역할” 단원을 참조하십시오.

이 정책은 서비스 연결 역할이 Security Hub CSPM 제어에 대한 보안 검사와 같은 태스크를 수행할 수 있도록 하는 관리 권한을 부여합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `cloudtrail` – CloudTrail 추적에 대한 정보를 검색합니다.
- `cloudwatch` - 현재 CloudWatch 경보 및 커넥터 상태 지표를 검색합니다.
- `logs` – CloudWatch 로그의 지표 필터를 검색합니다.
- `sns` – SNS 주제에 대한 구독 목록을 검색합니다.
- `config` - 구성 레코더, 리소스 및 AWS Config 규칙에 대한 정보를 검색합니다. Security Hub CSPM 서비스 연결 구성 레코더 및 타사 서비스 연결 구성 레코더를 관리합니다. AWS Config 규칙을 생성 및 삭제하고 규칙에 대한 평가를 실행합니다. 구성 레코더를 나열하고 타사 클라우드 통합을 지원하는 커넥터 정보를 가져옵니다.
- `iam` - 계정에 대한 자격 증명 보고서를 검색 및 생성하고에 대한 서비스 연결 역할을 생성합니다 AWS Config.

- `organizations` – 조직의 계정 및 OU(조직 단위) 정보를 검색합니다.
- `securityhub` – Security Hub CSPM 서비스, 표준 및 제어가 구성된 방식에 대한 정보를 검색합니다.
- `tag` – 리소스 태그에 대한 정보를 검색합니다.

이 정책의 권한을 검토하려면 AWS 관리형 정책 참조 안내서의 AWSSecurityHubServiceRolePolicy를 참조하세요.

AWS 관리형 정책에 대한 Security Hub 업데이트

다음 표에는이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 AWS Security Hub 및 Security Hub CSPM의 AWS 관리형 정책 업데이트에 대한 세부 정보가 나와 있습니다. 이 정책의 업데이트에 대한 자동 알림을 받으려면 Security Hub 문서 기록 페이지에서 RSS 피드를 구독하세요.

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubServiceRolePolicy – 업데이트된 정책 | Security Hub CSPM은 타사 통합을 지원하도록 정책을 업데이트했습니다. 업데이트에 타사 구성 레코더 관리, 구성 레코더 나열, 커넥터 정보 가져오기, 커넥터 상태 지표 검색 권한이 추가되었습니다. | 2026년 6월 30일 |
| AWSSecurityHubServiceRolePolicy – 업데이트된 정책 | Security Hub CSPM은 Security Hub CSPM 서비스 연결 구성 레코더를 관리하고 AWS Config 서비스 연결 역할을 생성할 수 있는 권한을 추가하도록 정책을 업데이트했습니다. | 2026년 4월 29일 |
| AWSSecurityHubOrganizationsAccess – 업데이트된 정책 | Security Hub는 Security Hub 기능을 지원하는 리소스 정책을 설명하는 권한을 추가하도 | 2025년 11월 12일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| | 록 정책을 업데이트했습니다. Security Hub는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. | |
| AWSSecurityHubFullAccess – 업데이트된 정책 | Security Hub는 Security Hub 기능을 지원하기 위해 GuardDuty, Amazon Inspector 및 계정 관리 관리에 대한 기능을 추가하도록 정책을 업데이트했습니다. Security Hub는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. | 2025년 11월 17일 |
| AWSSecurityHubOrganizationsAccess – 기존 정책 업데이트 | Security Hub는 정책에 대한 새로운 권한을 추가했습니다. 이러한 권한을 통해 조직 관리는 조직의 Security Hub 및 Security Hub CSPM을 활성화하고 관리할 수 있습니다. | 2025년 6월 17일 |
| AWSSecurityHubFullAccess – 기존 정책 업데이트 | Security Hub CSPM은 위탁자가 Security Hub에 대한 서비스 연결 역할을 생성할 수 있는 새 권한을 추가했습니다. | 2025년 6월 17일 |
| AWSSecurityHubFullAccess – 기존 정책 업데이트 | Security Hub CSPM은 AWS 서비스 및 제품에 대한 요금 세부 정보를 가져오도록 정책을 업데이트했습니다. | 2024년 4월 24일 |
| AWSSecurityHubReadOnlyAccess – 기존 정책 업데이트 | Security Hub CSPM은 `Sid` 필드를 추가하여 이 관리형 정책을 업데이트했습니다. | 2024년 2월 22일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubFullAccess – 기존 정책 업데이트 | Security Hub CSPM은 Amazon GuardDuty 및 Amazon Inspector가 계정에서 활성화되어 있는지 확인할 수 있도록 정책을 업데이트했습니다. 이를 통해 고객은 여러에서 보안 관련 정보를 통합할 수 있습니다 AWS 서비스. | 2023년 11월 16일 |
| AWSSecurityHubOrganizationsAccess – 기존 정책 업데이트 | Security Hub CSPM은 AWS Organizations 위임된 관리자 기능에 대한 읽기 전용 액세스를 허용하는 추가 권한을 부여하도록 정책을 업데이트했습니다. 여기에는 루트, 조직 단위(OU), 계정, 조직 구조 및 서비스 액세스와 같은 세부 정보가 포함됩니다. | 2023년 11월 16일 |
| AWSSecurityHubServiceRolePolicy – 기존 정책 업데이트 | Security Hub CSPM은 사용자 지정 가능한 보안 제어 속성을 읽고 업데이트할 수 있는 `BatchGetSecurityControls` , `DisassociateFromAdministratorAccount` 및 `UpdateSecurityControl` 권한을 추가했습니다. | 2023년 11월 26일 |
| AWSSecurityHubServiceRolePolicy – 기존 정책 업데이트 | Security Hub CSPM은 조사 결과와 관련된 리소스 태그를 읽을 수 있는 `tag:GetResources` 권한을 추가했습니다. | 2023년 11월 7일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubServiceRolePolicy – 기존 정책 업데이트 | Security Hub CSPM은 표준에서 제어의 활성화 상태에 대한 정보를 가져올 수 있는 `BatchGetStandardsControlAssociations` 권한을 추가했습니다. | 2023년 9월 27일 |
| AWSSecurityHubServiceRolePolicy – 기존 정책 업데이트 | Security Hub CSPM은 표준 및 제어를 포함하여 AWS Organizations 데이터를 가져오고 Security Hub CSPM 구성을 읽고 업데이트할 수 있는 새로운 권한을 추가했습니다. | 2023년 9월 20일 |
| AWSSecurityHubServiceRolePolicy – 기존 정책 업데이트 | Security Hub CSPM은 기존 `config:DescribeConfigRuleEvaluationStatus` 권한을 이 정책 내의 다른 설명으로 옮겼습니다. 이제 `config:DescribeConfigRuleEvaluationStatus` 권한이 모든 리소스에 적용됩니다. | 2023년 3월 17일 |
| AWSSecurityHubServiceRolePolicy – 기존 정책 업데이트 | Security Hub CSPM은 기존 `config:PutEvaluations` 권한을 이 정책 내의 다른 설명으로 옮겼습니다. 이제 `config:PutEvaluations` 권한이 모든 리소스에 적용됩니다. | 2021년 7월 14일 |

| 변경 | 설명 | Date |
| --- | --- | --- |
| AWSSecurityHubServiceRolePolicy – 기존 정책 업데이트 | Security Hub CSPM은 서비스 연결 역할이 평가 결과를 AWS Config에 제공할 수 있는 새로운 권한을 추가했습니다. | 2021년 6월 29일 |
| AWSSecurityHubServiceRolePolicy – 관리형 정책 목록에 추가했습니다. | Security Hub CSPM 서비스 연결 역할에서 사용하는 관리형 정책인 AWSSecurityHubServiceRolePolicy에 관한 정보가 추가되었습니다. | 2021년 6월 11일 |
| AWSSecurityHubOrganizationsAccess – 새로운 정책 | Security Hub CSPM은 Security Hub CSPM과 Organizations의 통합에 필요한 권한을 부여하는 새로운 정책을 추가했습니다. | 2021년 3월 15일 |
| Security Hub CSPM이 변경 내용 추적을 시작했습니다 | Security Hub CSPM이 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다. | 2021년 3월 15일 |

## AWS Security Hub CSPM 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단 AWS Security Hub CSPM 하고 수정할 수 있습니다.

주제

- Security Hub CSPM에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- Security Hub CSPM에 프로그래밍 방식으로 액세스하고 싶습니다.
- 관리자인데 다른 사용자가 Security Hub CSPM에 액세스하도록 허용하려고 함
- 내 외부의 사람이 내 Security Hub CSPM 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

Security Hub CSPM에서 작업을 수행할 권한이 없음

에서 작업을 수행할 권한이 없다는 AWS Management Console 메시지가 표시되면 관리자에게 문의하여 도움을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 사용자 `mateojackson`이 콘솔을 사용하여 *##*에 대한 세부 정보를 보려고 하지만 `securityhub:`*`GetWidget`* 권한이 없는 경우에 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 securityhub:GetWidget on resource: my-example-widget
```

이 경우, Mateo는 *`my-example-widget`* 작업을 사용하여 `securityhub:`*`GetWidget`* 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Security Hub에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Security Hub에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

Security Hub CSPM에 프로그래밍 방식으로 액세스하고 싶습니다.

사용자는 AWS 외부에서와 상호 작용하려는 경우 프로그래밍 방식으로 액세스해야 합니다 AWS Management Console. 프로그래밍 방식 액세스를 부여하는 방법은에 액세스하는 사용자 유형에 따라 다릅니다 AWS.

사용자에게 프로그래밍 방식 액세스 권한을 부여하려면 다음 옵션 중 하나를 선택합니다.

| 프로그래밍 방식 액세스가 필요한 사용자 | 목적 | 방법 |
| --- | --- | --- |
| IAM | (권장) 콘솔 자격 증명을 임시 자격 증명으로 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다.<br>• 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 AWS 로컬 개발을 위한 로그인을 참조하세요.<br>• AWS SDKs 경우 SDK 및 도구 참조 안내서의 AWS 로컬 개발을 위한 로그인을 참조하세요. AWS SDKs |
| 작업 인력 ID<br><br>(IAM Identity Center에서 관리되는 사용자) | 임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다.<br>• 자세한 AWS CLI내용은 AWS Command Line Interface 사용 설명서의 AWS CLI 를 사용하도록 구성을 AWS IAM Identity Center 참조하세요.<br>• AWS SDKs, 도구 및 AWS APIs 경우 SDK 및 도구 참조 안내서의 IAM Identity Center 인증을 참조하세요. AWS SDKs |
| IAM | 임시 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | IAM 사용 설명서의 AWS 리소스에서 임시 자격 증명 사용의 지침을 따릅니다. |
| IAM | (권장되지 않음) | 사용하고자 하는 인터페이스에 대한 지침을 따릅니다. |

| 프로그래밍 방식 액세스가 필요한 사용자 | 목적 | 방법 |
| --- | --- | --- |
| | 장기 자격 증명을 사용하여 AWS CLI, AWS SDKs 또는 AWS APIs. | • 자세한 AWS CLI내용은 사용 AWS Command Line Interface 설명서의 IAM 사용자 자격 증명을 사용하여 인증을 참조하세요.<br>• AWS SDKs 및 도구의 경우 SDK 및 도구 참조 안내서의 장기 자격 증명을 사용하여 인증을 참조하세요. AWS SDKs<br>• AWS APIs 경우 IAM 사용 설명서의 IAM 사용자의 액세스 키 관리를 참조하세요. |

관리자인데 다른 사용자가 Security Hub CSPM에 액세스하도록 허용하려고 함

액세스 권한을 제공하려면 사용자, 그룹 또는 역할에 권한을 추가하세요.

- 의 사용자 및 그룹 AWS IAM Identity Center:

  권한 세트를 생성합니다. AWS IAM Identity Center 사용자 안내서에서 권한 세트 생성의 지침을 따릅니다.
- ID 제공업체를 통해 IAM에서 관리되는 사용자:

  ID 페더레이션을 위한 역할을 생성합니다. IAM 사용자 설명서의 Create a role for a third-party identity provider (federation)의 지침을 따릅니다.
- IAM 사용자:
  - 사용자가 맡을 수 있는 역할을 생성합니다. IAM 사용자 설명서에서 Create a role for an IAM user의 지침을 따릅니다.
  - (권장되지 않음) 정책을 사용자에게 직접 연결하거나 사용자를 사용자 그룹에 추가합니다. IAM 사용 설명서에서 사용자(콘솔)에 권한 추가의 지침을 따릅니다.

내 외부의 사람이 내 Security Hub CSPM 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Security Hub에서 이러한 기능을 지원하는지 여부를 알아보려면 IAM에서 Security Hub의 작동 방식 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

## 에 대한 규정 준수 검증 AWS Security Hub CSPM

새로운 AWS 가입 환경은 규제 워크로드용으로 설계되지 않았습니다. 새로운 AWS 가입 환경을 사용하고 있지만 규제 대상 워크로드 AWS 에를 사용하려는 경우 AWS 환경에 가입 AWS (고급)하거나 고급 기능을 활성화할 수 있습니다.

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 제공 범위 내를 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다. 사용 시 규정 준수 책임에 대한 자세한 내용은 AWS 보안 설명서를 AWS 서비스참조하세요.

# AWS Security Hub의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며, 이러한 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크를 통해 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

# 의 인프라 보안 AWS Security Hub CSPM

관리형 서비스인는 AWS 글로벌 네트워크 보안으로 보호 AWS Security Hub CSPM 됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요 AWS .

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Security Hub CSPM에 액세스합니다. 클라이언트는 다음을 지원해야 합니다.

- Transport Layer Security(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

# AWS Security Hub CSPM 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성 AWS Security Hub CSPM 하여 VPC와 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이AWS PrivateLink, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 Security Hub CSPM APIs에 비공개로 액세스할 수 있는 기술로 구동됩니다. VPC의 인스턴스는 Security Hub CSPM APIs. VPC와 Security Hub CSPM 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 Elastic Network Interfaces로 표현됩니다. 자세한 내용은 Amazon Virtual Private Cloud 가이드의 인터페이스 VPC 엔드포인트를 AWS 서비스 사용하여 액세스를 참조하세요.

## Security Hub CSPM VPC 엔드포인트에 대한 고려 사항

Security Hub CSPM에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon Virtual Private Cloud 가이드의 사전 조건 및 기타 정보를 검토해야 합니다.

Security Hub CSPM은 VPC에서 모든 API 작업을 호출할 수 있도록 지원합니다.

## Security Hub CSPM용 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 Security Hub CSPM 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 Amazon Virtual Private Cloud 설명서의 VPC 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 Security Hub CSPM용 VPC 엔드포인트를 생성합니다.

`com.amazonaws.region.securityhub`

여기서 *region*은 해당 AWS 리전의 리전 코드입니다.

엔드포인트에 대해 프라이빗 DNS를 활성화하는 경우 미국 동부(버지니아 북부) 리전과 같은 리전의 기본 DNS 이름을 사용하여 Security Hub CSPM`securityhub.us-east-1.amazonaws.com`에 API 요청을 할 수 있습니다.

## Security Hub CSPM에 대한 VPC 엔드포인트 정책 생성

Security Hub CSPM에 대한 액세스를 제어하는 VPC 엔드포인트에 엔드포인트 정책을 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스

자세한 내용은 Amazon Virtual Private Cloud 설명서의 엔드포인트 정책을 사용한 VPC 엔드포인트에 대한 액세스 제어를 참조하세요.

예: Security Hub CSPM 작업에 대한 VPC 엔드포인트 정책

다음은 Security Hub CSPM에 대한 엔드포인트 정책의 예입니다. 엔드포인트에 연결되면이 정책은 모든 리소스의 모든 보안 주체에 대해 나열된 Security Hub CSPM 작업에 대한 액세스 권한을 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securityhub:getFindings",
            "securityhub:getEnabledStandards",
            "securityhub:getInsights"
         ],
         "Resource":"*"
      }
   ]
}
```

### 공유 서브넷

공유하는 서브넷의 VPC 엔드포인트는 생성, 설명, 수정 또는 삭제할 수 없습니다. 그러나 공유하는 서브넷의 VPC 엔드포인트를 사용할 수는 있습니다. VPC 공유에 대한 자세한 내용은 Amazon Virtual Private Cloud 설명서의 다른 계정과 VPC 서브넷 공유를 참조하세요.

## CloudTrail을 사용하여 Security Hub API 직접 호출 로깅

AWSSecurity Hub CSPM은 Security Hub CSPM에서 사용자AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS서비스와 통합됩니다. CloudTrail은 Security Hub CSPM에 대한 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 직접 호출에는 Security Hub CSPM 콘솔에서 수행한 직접 호출과 Security Hub CSPM API 작업에 대한 코드 직접 호출이 포함됩니다. 추적을 생성하면 Security Hub CSPM 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail이 수집한 정보를 사용하여 Security Hub CSPM에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 활성화 방법을 포함하여 CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용자 안내서를 참조하세요.

### CloudTrail의 Security Hub CSPM 정보

CloudTrail은 계정을 생성할 AWS 계정때에서 활성화됩니다. Security Hub CSPM에서 지원되는 이벤트 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS서비스 이벤트와 함께 CloudTrail 이벤트에

기록됩니다. 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Security Hub CSPM에 대한 이벤트를 포함하여 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 추가적으로, CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

Security Hub CSPM은 모든 Security Hub CSPM API 작업을 CloudTrail 로그에 이벤트로 로깅하는 것을 지원합니다. Security Hub CSPM 작업 목록을 보려면 Security Hub CSPM API 참조를 참조하세요.

다음 작업에 대한 작업이 CloudTrail에 로깅될 때 `responseElements`의 값은 `null`로 설정됩니다. 이렇게 하면 민감한 정보가 CloudTrail 로그에 포함되지 않습니다.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 이루어졌는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 요청이 다른 AWS서비스에서 이루어졌는지 여부

자세한 내용은 CloudTrail userIdentity 요소를 참조하세요.

# 예제: Security Hub CSPM 로그 파일 항목

트레일이란 지정한 S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `CreateInsight` 작업을 보여주는 CloudTrail 로그 항목이 나타냅니다. 이 예제에서는 `Test Insight`라는 인사이트가 생성됩니다. `ResourceId` 속성은 그룹화 기준 집계자로 지정되며 이 인사이트를 위한 선택적 필터는 지정되지 않습니다. 인사이트에 대한 자세한 내용은 Security Hub CSPM에서 인사이트 보기 섹션을 참조하세요.


```
{
    "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"
```

```
}
```

# Security Hub 리소스 태그 지정

태그는 특정 유형의 AWSSecurity Hub CSPM AWS리소스를 포함하여 리소스에 정의하고 할당할 수 있는 선택적 레이블입니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별하고, 분류하고 관리하는 데 도움이 됩니다. 예를 들어, 태그를 사용하여 리소스를 구분하고, 특정 규정 준수 요구 사항 또는 워크플로를 지원하는 리소스를 식별하거나, 비용을 할당할 수 있습니다.

태그를 추가할 수 있는 Security Hub CSPM 리소스 유형은 다음과 같습니다.

- 자동화 규칙
- 구성 정책
- Hub 리소스

## 태그 지정 기본 사항

리소스는 최대 50개의 태그를 가질 수 있습니다. 각 태그는 사용자가 정의하는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그 키는 더 구체적인 태그 값에 대해 카테고리와 같은 역할을 하는 일반적인 레이블입니다. 태그 값은 태그 키에 대한 설명자 역할을 합니다.

예를 들어, 환경마다 다른 자동화 규칙(테스트 계정용 자동화 규칙 세트 하나, 프로덕션 계정용 자동화 규칙 세트 하나)을 만드는 경우, 해당 규칙에 `Environment` 태그 키를 할당할 수 있습니다. 관련 태그 값은 테스트 계정과 연결된 규칙의 경우 `Test`이고 프로덕션 계정 및 OU와 연결된 규칙의 경우, `Prod`일 수 있습니다.

AWSSecurity Hub CSPM 리소스를 정의하고 태그를 할당할 때 다음 사항에 유의하세요.

- 각 리소스는 최대 50개의 태그를 보유할 수 있습니다.
- 각 리소스에 대해 각 태그 키는 고유하며 하나의 태그 값만 가질 수 있습니다.
- 태그 키와 값은 대소문자를 구분합니다. 모범적으로는 태그를 대문자로 사용하는 전략을 세우고 이러한 전략을 모든 리소스 유형에 대해 일관되게 구현하는 것이 좋습니다.
- 태그 키는 최대 128개의 UTF-8 문자를 포함할 수 있습니다. 태그 값은 최대 256개의 UTF-8 문자를 포함할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.
- `aws:` 접두사는에서 사용하도록 예약되어 있습니다AWS. 정의한 태그 키나 값에는 이를 사용할 수 없습니다. 또는 이 접두사를 사용하는 태그 키 또는 값을 변경하거나 제거할 수 없습니다. 이 접두사를 사용하는 태그는 리소스당 50개의 할당량에 포함되지 않습니다.

- 할당하는 모든 태그는 에서만 사용할 수 AWS 계정있으며 할당하는 AWS 리전에서만 사용할 수 있습니다.
- Security Hub CSPM을 사용하여 리소스에 태그를 할당하는 경우, 해당 태그는 해당 AWS 리전의 Security Hub CSPM에 직접 저장된 리소스에만 적용됩니다. Security Hub CSPM이 다른 AWS 서비스에서 생성, 사용 또는 유지 관리하는 연결된 지원 리소스에는 적용되지 않습니다. 예를 들어, Amazon Simple Storage Service(Amazon S3)와 관련된 조사 결과를 업데이트하는 자동화 규칙에 태그를 할당하는 경우, 태그는 지정된 리전의 Security Hub CSPM에 있는 자동화 규칙에만 적용됩니다. S3 버킷에는 적용되지 않습니다. 연결된 리소스에 태그를 할당하려면 S3 버킷의 Amazon S3와 같이 리소스를 AWS 서비스저장하는 AWS Resource Groups또는를 사용할 수 있습니다. S3 관련 리소스에 태그를 할당하면 Security Hub CSPM 리소스에 대한 지원 리소스를 식별하는 데 도움이 될 수 있습니다.
- 리소스를 삭제하면, 리소스에 지정된 태그 또한 삭제됩니다.

> **Important**
>
> 기밀 또는 기타 유형의 민감한 데이터를 태그에 저장하지 마세요. 를 AWS 서비스포함하여 많은에서 태그에 액세스할 수 있습니다AWS 결제 및 비용 관리. 태그는 민감한 데이터에 사용하기 위한 것이 아닙니다.

Security Hub CSPM 리소스에 대한 태그를 추가하고 관리하려면 Security Hub CSPM 콘솔, Security Hub CSPM API 또는 AWS Resource Groups태깅 API를 사용할 수 있습니다. Security Hub CSPM을 사용하면 리소스를 생성할 때 태그를 리소스에 추가할 수 있습니다. 개별 기존 리소스의 태그를 추가하고 관리할 수도 있습니다. Resource Groups를 사용하면 Security Hub CSPM을 AWS 서비스포함하여 여러에 걸쳐 있는 여러 기존 리소스에 대해 태그를 대량으로 추가하고 관리할 수 있습니다.

추가 태그 지정 팁과 모범 사례는 AWS리소스 태그 지정 사용 설명서의 리소스 태그 지정을 참조하세요. AWS

## IAM 정책에서 태그 사용

리소스에 태그를 지정한 후 AWS Identity and Access Management(IAM)정책에서 태그 기반의 리소스 수준 권한을 정의할 수 있습니다. 이러한 방식으로 태그를 사용하면 리소스를 생성하고 태그를 지정할 AWS 계정권한이 있는의 사용자 및 역할과 태그를 더 일반적으로 추가, 편집 및 제거할 권한이 있는 사용자 및 역할에 대한 세분화된 제어를 구현할 수 있습니다. 태그를 기반으로 액세스를 컨트롤하려면 IAM 정책의 조건 요소에서 태그 관련 조건 키를 사용하면 됩니다.

예를 들어, 리소스에 대한 Owner 태그가 사용자 이름을 지정하는 경우, 사용자가 모든 AWS Security Hub CSPM 리소스에 대한 전체 액세스 권한을 갖도록 허용하는 IAM 정책을 생성할 수 있습니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securityhub:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner":
 "${aws:username}"}
            }
        }
    ]
}
```

태그 기반의 리소스 수준 권한을 정의하면 권한이 즉시 적용됩니다. 즉, 리소스를 생성하자마자 더 안전하게 보호할 수 있으며 새로운 리소스에 태그 사용 적용을 빠르게 시작할 수 있습니다. 리소스 수준 권한을 사용하여 새로운 및 기존 리소스와 연결할 수 있는 태그 키와 값을 제어할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 태그를 사용하여 AWS리소스에 대한 액세스 제어를 참조하세요.

## Security Hub CSPM 리소스에 태그 추가

태그는 특정 유형의 AWSSecurity Hub CSPM AWS리소스를 포함하여 리소스를 정의하고 리소스에 할당할 수 있는 레이블입니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 식별, 분류, 관리하는 데 도움이 됩니다. 예를 들어 태그를 사용하여 정책을 적용하고, 비용을 할당하고, 리소스 버전을 구분하거나, 특정 규정 준수 요구 사항 또는 워크플로를 지원하는 리소스를 식별할 수 있습니다.

태그를 추가할 수 있는 Security Hub CSPM 리소스 유형은 다음과 같습니다.

- 자동화 규칙
- 구성 정책

- Hub 리소스

리소스는 최대 50개의 태그를 가질 수 있습니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그 키는 더 구체적인 태그 값에 대해 카테고리와 같은 역할을 하는 일반적인 레이블입니다. 태그 값은 태그 키에 대한 설명자 역할을 합니다. 태그 지정 옵션과 요구 사항에 대한 자세한 내용은 태그 지정 기본 사항 섹션을 참조하세요.

Security Hub CSPM 리소스에 태그를 추가하려면 Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용할 수 있습니다. 콘솔은 Hub 리소스에 태그를 추가하는 것을 지원하지 않습니다.

태그를 추가한 후 태그를 편집하고 태그 키 또는 태그 값을 변경할 수 있습니다.

여러 Security Hub CSPM 리소스의 태그를 동시에 편집하려면 AWS Resource Groups Tagging API의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스에 태그를 추가하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 리소스에 태그를 추가하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management(IAM) 정책을 검토합니다.

Console

Security Hub CSPM 리소스에 태그를 추가하려면(콘솔)

자동화 규칙 또는 구성 정책을 만들면 Security Hub CSPM 콘솔에서 태그를 추가할 수 있는 옵션을 제공합니다. 태그 섹션에서 태그 키와 태그 값을 제공할 수 있습니다.

Security Hub CSPM API

Security Hub CSPM 리소스에 태그를 추가하려면(API)

리소스를 만들고 프로그래밍 방식으로 하나 이상의 태그를 추가하려면 만들려는 리소스 유형에 적합한 작업을 사용하세요.

- 구성 정책을 만들고 여기에 하나 이상의 태그를 추가하려면 CreateConfigurationPolicy API를 호출하거나, AWS CLI를 사용하는 경우, create-configuration-policy 명령을 실행합니다.
- 자동화 규칙을 생성하고 여기에 하나 이상의 태그를 추가하려면 CreateAutomationRule API를 호출하거나, AWS CLI를 사용하는 경우, create-automation-rule 명령을 실행하세요.

- Security Hub CSPM을 활성화하고 Hub 리소스에 하나 이상의 태그를 추가하려면 EnableSecurityHub API를 간접적으로 호출하거나, AWS Command Line Interface(AWS CLI)를 사용하는 경우 enable-security-hub 명령을 실행합니다.

요청에서 `tags` 파라미터를 사용하여 리소스에 추가할 각 태그의 태그 키와 선택적 태그 값을 지정합니다. `tags` 파라미터는 객체 배열을 지정합니다. 각 객체는 태그 키 및 연결된 태그 값을 지정합니다.

기존 리소스에 하나 이상의 태그를 추가하려면 Security Hub CSPM API의 TagResource 작업을 사용하거나를 사용하는 경우 tag-resource 명령을 AWS CLI실행합니다. 요청에서 태그를 추가하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. `tags` 파라미터를 사용하여 추가할 각 태그의 태그 키(`key`)와 선택적 태그 값(`value`)을 지정합니다. `tags` 파라미터는 객체의 배열, 각 태그 키당 하나의 개체 및 관련 태그 값을 지정합니다.

예를 들어 다음 AWS CLI명령은 지정된 구성 정책에 `Environment` 태그 값이 있는 `Prod` 태그 키를 추가합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

CLI 명령 예제:

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Prod"}'
```

위치:

- `resource-arn`은 태그를 추가할 구성 정책의 ARN을 지정합니다.
- *`Environment`*은 규칙에 추가할 태그의 태그 키입니다.
- *`Prod`*은 지정된 태그 키의 태그 값입니다(*`Environment`*).

다음 예제에서 명령은 구성 정책에 여러 태그를 추가합니다.

```
$ 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"}'
```

`tags` 배열의 각 개체에는 `key` 및 `value` 인수가 모두 필요합니다. 그러나 `value` 인수 값은 빈 문자열일 수도 있습니다. 태그 값을 태그 키와 연결하지 않으려면 `value` 인수 값을 지정하지 마세요. 예를 들어, 다음 명령은 관련 태그 값이 없는 `Owner` 태그 키를 추가합니다.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

태그 지정 작업이 성공하면 Security Hub CSPM은 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Hub CSPM은 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

## Security Hub CSPM 리소스의 태그 편집

시간이 지남에 따라 환경 또는 요구 사항이 변경되면 AWSSecurity Hub CSPM 리소스의 기존 태그를 평가하고 필요에 따라 태그를 변경할 수 있습니다. 태그는 특정 유형의 Macie 리소스를 포함한 AWS 리소스를 선택적으로 정의하고 연결하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그 키는 더 구체적인 태그 값에 대해 카테고리와 같은 역할을 하는 일반적인 레이블입니다. 태그 값은 태그 키에 대한 설명자 역할을 합니다.

태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 분류하고 관리하는 데 도움이 됩니다. 예를 들어 태그를 사용하여 정책을 적용하고, 비용을 할당하고, 리소스 버전을 구분하거나, 특정 규정 준수 요구 사항 또는 워크플로를 지원하는 리소스를 식별할 수 있습니다.

태그를 추가할 수 있는 Security Hub CSPM 리소스 유형은 다음과 같습니다.

- 자동화 규칙
- 구성 정책
- Hub 리소스

Security Hub CSPM 리소스의 태그 키 또는 태그 값을 편집하려면 Security Hub CSPM API를 사용할 수 있습니다. Security Hub CSPM 콘솔은 현재 태그 편집을 지원하지 않습니다.

> **Important**
>
> 리소스의 태그를 편집하면 리소스 액세스에 영향을 미칠 수 있습니다. 리소스에 대한 태그를 편집하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 모든 AWS Identity and Access Management(IAM) 정책을 검토하세요.

### Security Hub CSPM API

#### Security Hub CSPM 리소스의 태그를 편집하려면(API)

프로그래밍 방식으로 리소스의 태그를 편집하면 기존 태그를 새로운 값으로 덮어쓰게 됩니다. 따라서 태그를 편집하는 가장 좋은 방법은 태그 키를 편집할지, 태그 값을 편집할지 또는 둘 다를 편집할지에 따라 달라집니다. 태그 키를 편집하려면 현재 태그를 제거하고 새로운 태그를 추가합니다.

태그 키와 연결된 태그 값만 편집하거나 제거하려면 Security Hub CSPM API의 TagResource 작업을 사용하여 기존 값을 덮어씁니다. AWS CLI를 사용하는 경우, tag-resource 명령을 실행하세요. 요청에서 태그 값을 편집하거나 제거하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

태그 값을 편집하려면 `tags` 파라미터를 사용하여 태그 값을 변경하려는 태그 키를 지정합니다. 또한 키에 새로운 태그 값을 지정해야 합니다. 예를 들어 다음 AWS CLI명령은 지정된 자동화 규칙에 할당된 태그 키`ProdTest`의 `Environment` 태그 값을에서 로 변경합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securityhub tag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Environment":"Test"}'
```

위치:

- `resource-arn`은 구성 정책의 ARN을 지정합니다.
- *`Environment`*는 변경할 태그 값과 연결된 태그 키입니다.
- *`Test`*는 지정된 태그 키(*`Environment`*)에 사용할 새로운 태그 값입니다.

태그 키에서 태그 값을 제거하려면 `tags` 파라미터에 키 `value` 인수 값을 지정하지 마세요. 예제:

```
$ aws securityhub tag-resource \
```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tags '{"Owner":""}'
```

작업이 성공하면 Security Hub CSPM은 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Hub CSPM은 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

# Security Hub CSPM 리소스에 대한 태그 검토

AWSSecurity Hub CSPM 리소스에 대한 태그를 추가하거나 편집한 후 리소스에 현재 있는 태그 키와 태그 값을 볼 수 있습니다. 태그는 특정 유형의 Macie 리소스를 포함한 AWS 리소스를 선택적으로 정의하고 연결하는 레이블입니다. 각 태그는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그 키는 더 구체적인 태그 값에 대해 카테고리와 같은 역할을 하는 일반적인 레이블입니다. 태그 값은 태그 키에 대한 설명자 역할을 합니다.

태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 분류하고 관리하는 데 도움이 됩니다. 예를 들어 태그를 사용하여 정책을 적용하고, 비용을 할당하고, 리소스 버전을 구분하거나, 특정 규정 준수 요구 사항 또는 워크플로를 지원하는 리소스를 식별할 수 있습니다.

태그를 추가할 수 있는 Security Hub CSPM 리소스 유형은 다음과 같습니다.

- 자동화 규칙
- 구성 정책
- Hub 리소스

Security Hub CSPM 콘솔 또는 Security Hub CSPM API를 사용하여 Security Hub CSPM 자동화 규칙 또는 구성 정책의 태그를 검토할 수 있습니다. 콘솔은 Hub 리소스에 대한 태그 검토를 지원하지 않습니다. 프로그래밍 방식으로 모든 리소스의 태그를 검토할 수 있습니다.

여러 Security Hub CSPM 리소스의 태그를 동시에 검토하려면 AWS Resource Groups Tagging API의 태그 지정 작업을 사용합니다.

Console

Security Hub CSPM 리소스의 태그를 검토하려면(콘솔)

1. Security Hub CSPM 관리자의 자격 증명을 사용하여 https://console.aws.amazon.com/securityhub/ AWSSecurity Hub CSPM 콘솔을 엽니다.

2. 태그를 추가하고 싶은 리소스 유형에 따라 다음 중 하나를 수행합니다.

   - 자동화 규칙의 태그를 검토하려면 탐색 창에서 자동화를 선택합니다. 그런 다음 자동화 규칙을 선택합니다.
   - 구성 정책의 태그를 검토하려면 탐색 창에서 구성을 선택합니다. 그런 다음 정책 탭에서 구성 정책 옆에 있는 옵션을 선택합니다. 정책에 할당된 태그 수를 보여주는 사이드 패널이 열립니다. 태그 헤더를 확장하여 태그 키와 태그 값을 볼 수 있습니다.

태그 섹션에는 현재 리소스에 할당된 모든 태그가 나열됩니다.

Security Hub CSPM API

Security Hub CSPM 리소스의 태그를 검토하려면(API)

기존 리소스의 태그를 검색하고 검토하려면 ListTagsForResource API를 호출하세요. 요청에서 `resourceArn` 파라미터를 사용하여 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

를 사용하는 경우 list-tags-for-resource 명령을 AWS CLI실행하고 `resource-arn` 파라미터를 사용하여 리소스의 ARN을 지정합니다. 예제:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

작업이 성공하면 Security Hub CSPM은 `tags` 배열을 반환합니다. 배열의 각 객체는 현재 리소스에 할당된 태그 (태그 키와 태그 값 모두)를 지정합니다. 예제:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Prod"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
    ]
```

```
}
```

여기서 Environment, CostCenter, Owner는 리소스에 할당된 태그 키입니다. Prod는 Environment 태그 키에 연결된 태그 값입니다. 12345는 CostCenter 태그 키에 연결된 태그 값입니다. Owner 태그 키에 연결된 태그 값이 없습니다.

태그가 있는 모든 Security Hub CSPM 리소스 목록과 각 리소스에 할당된 모든 태그를 검색하려면 AWS Resource Groups태깅 API의 GetResources 작업을 사용합니다. 요청에서 ResourceTypeFilters 파라미터 값을 securityhub로 설정합니다. 를 사용하여 이렇게 하려면 get-resources 명령을 AWS CLI실행하고 resource-type-filters 파라미터 값을 로 설정합니다securityhub. 예제:

```
$ aws resourcegroupstaggingapi get-resources -\-resource-type-filters "securityhub"
```

작업이 성공하면 Resource Groups가 ResourceTagMappingList 배열을 반환합니다. 배열에는 태그가 있는 각 Security Hub CSPM 리소스에 대해 하나의 객체가 포함됩니다. 각 객체는 Security Hub CSPM 리소스의 ARN과 해당 리소스에 할당된 태그 키 및 값을 지정합니다.

## Security Hub CSPM 리소스에서 태그 제거

AWSSecurity Hub CSPM 리소스에 태그를 추가하는 경우 나중에 하나 이상의 태그를 제거할 수 있습니다. 태그는 특정 유형의 Security Hub CSPM 리소스를 포함한 AWS 리소스에 정의하고 할당하는 레이블입니다. 자동화 규칙, 구성 정책, Hub 리소스 등 Security Hub CSPM 리소스 유형에 다음 태그를 추가, 편집, 제거할 수 있습니다.

개별 AWSSecurity Hub CSPM 리소스에서 태그를 제거하려면 Security Hub CSPM API를 사용하면 됩니다. Security Hub CSPM 콘솔은 현재 태그 제거를 지원하지 않습니다.

여러 Security Hub CSPM 리소스에서 태그를 동시에 제거하려면 AWS Resource Groups Tagging API의 태그 지정 작업을 사용합니다.

> **Important**
>
> 리소스에서 태그를 제거하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 태그를 제거하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 AWS Identity and Access Management(IAM) 정책을 검토합니다.

Security Hub CSPM API

### Security Hub CSPM 리소스에서 태그를 제거하려면(API)

리소스에서 하나 이상의 태그를 프로그래밍 방식으로 삭제하려면 Security Hub CSPM API의 UntagResource 작업을 사용합니다. 요청에서 `resourceArn` 파라미터를 사용하여 태그를 제거할 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. `tagKeys`파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 여러 태그를 제거하려면 제거할 각 태그의 `tagKeys` 파라미터와 인수를 앰퍼샌드(&)로 구분하여 추가합니다—예제: `tagKeys=key1&tagKeys=key2`. 리소스에서 특정 태그 값(태그 키 제외)만 제거하려면 태그를 제거하는 대신 태그를 편집하세요.

를 사용하는 경우 untag-resource 명령을 AWS CLI실행하여 리소스에서 하나 이상의 태그를 제거합니다. `resource-arn` 파라미터에는 태그를 제거할 리소스의 ARN을 지정합니다. `tag-keys`파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 예를 들어, 다음 명령은 지정된 구성 정책에서 `Environment` 태그(태그 키와 태그 값 모두)를 제거합니다.

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment
```

여기서 `resource-arn`은 태그를 제거할 구성 정책의 ARN을 지정하고, *`Environment`*는 제거할 태그의 태그 키입니다.

리소스에서 여러 태그를 제거하려면, 각 추가 키를 `tag-keys` 파라미터의 인수로 추가합니다. 예제:

```
$ aws securityhub untag-resource \
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \
--tag-keys Environment Owner
```

작업이 성공하면 Security Hub CSPM은 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Hub CSPM은 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

# Security Hub 할당량

AWS 계정에는 각각에 대해 이전에 제한이라고 하는 특정 기본 할당량이 있습니다AWS 서비스. 이러한 할당량은 한도라 함은 계정의 최대 서비스 리소스 또는 작업 수입니다. 이 주제는 계정의 AWSSecurity Hub 리소스 및 작업에 적용되는 할당량에 연결됩니다. 다르게 표시되지 않는 한, AWS 리전의 계정에 각 할당량이 적용됩니다.

일부 할당량만 늘릴 수 있습니다. 할당량 증가를 요청하려면 Service Quotas 콘솔을 사용합니다. 증가를 요청하는 방법을 알아보려면 Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요. Service Quotas 콘솔에서 할당량을 사용할 수 없는 경우의 서비스 한도 증가 양식을 사용하여 할당량 증가를 AWS Support Center Console요청합니다.

## 최대 할당량

AWS Security Hub 리소스에 적용되는 할당량 목록은 AWS 일반 참조의 AWS Security Hub 엔드포인트 및 할당량을 참조하세요.

## 비율 할당량

AWS Security Hub API 작업에 적용되는 할당량 목록은 AWS Security Hub API 참조를 참조하세요.

Security Hub CSPM에서 교차 리전 집계를 설정하는 경우 `BatchImportFindings` 및 `BatchUpdateFindings`를 한 번 직접적으로 호출하면 연결된 리전과 집계 영역에 영향을 미칩니다. 이 `GetFindings` 작업은 연결된 영역 및 집계 영역에서 조사 결과를 검색합니다. 하지만, `BatchEnableStandards` 및 `UpdateStandardsControl` 작업은 영역별로 다릅니다.

# AWS Security Hub 사용 설명서의 문서 기록

다음 표에서는 Security Hub 및 AWS Security Hub CSPM의 마지막 릴리스 이후 설명서에 대한 중요한 변경 사항을 설명합니다. 새 Security Hub CSPM 컨트롤 릴리스의 경우 날짜는 컨트롤이 지원되는에서 사용되기 시작하는 시기를 지정합니다 AWS 리전. 지원되는 모든 리전에서 제어를 사용할 수 있으려면 1~2주가 걸릴 수 있습니다. 기존 제어의 주요 변경 사항에 대한 자세한 내용은 Security Hub CSPM 제어의 변경 로그 섹션을 참조하세요.

이제 AWS Security Hub 사용 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

| 변경 사항 | 설명 | 날짜 |
| --- | --- | --- |
| 네트워크 스캔 정보 조사 결과 세부 정보 업데이트 | Network Scanning이 생성하는 정보 조사 결과에 대한 정보가 추가되었습니다. | 2026년 9월 3일 |
| 네트워크 스캔 포트 목록 업데이트 | 네트워크 스캔에서 현재 지원하는 포트 목록이 추가되었습니다. | 2026년 8월 18일 |
| 업데이트된 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에서 EFS.6 제어를 제거했습니다. 이 제어는 NIST SP 800-53 개정 5, NIST SP 800-171 개정 2 및 PCI DSS v4.0.1 표준에서 계속 사용할 수 있습니다. | 2026년 8월 3일 |
| 향상된 Security Hub 설명서 활성화 | AWS 조직 페이지에서 멤버 계정 구성 관리 페이지의 지침을 개선했습니다. | 2026년 7월 7일 |
| 네트워크 스캔 기능 설명서 추가 | Security Hub의 네트워크 스캔 기능에 대한 설명서 추가 | 2026년 7월 7일 |
| AI 인벤토리 | AWS 환경 전반의 관리형 및 자체 호스팅형 인공 지능(AI) 및 | 2026년 7월 7일 |

| | | |
|---|---|---|
| | 기계 학습(ML) 리소스에 대한 통합 보기를 제공하는 AI 인벤토리가 추가되었습니다. 자세한 내용은 AWS Security Hub의 AI 인벤토리를 참조하세요. | |
| 관리형 정책 업데이트 - AWSSecurityHubV2ServiceRolePolicy | Security Hub는 라는 AWS 관리형 정책을 업데이트했습니다AWSSecurityHubV2ServiceRolePolicy . 업데이트에는 타사 구성 레코더 관리, 커넥터 생성 및 관리, 페더레이션을 위한 웹 자격 증명 토큰 획득 등 타사 통합을 지원하는 권한이 추가되었습니다. | 2026년 6월 30일 |
| 관리형 정책 업데이트 - AWSSecurityHubServiceRolePolicy | Security Hub CSPM은 라는 AWS 관리형 정책을 업데이트했습니다AWSSecurityHubServiceRolePolicy . 업데이트에 타사 통합을 지원하는 권한이 추가되었습니다. 여기에는 타사 구성 레코더 관리 및 커넥터 상태 지표 검색이 포함됩니다. | 2026년 6월 30일 |
| 새로운 보안 표준 | Security Hub CSPM은 AI 보안 모범 사례 표준을 릴리스했습니다. 이 표준은 배포된 AI 리소스가 보안 모범 사례와 일치하지 않는 경우를 감지하는 엄선된 제어 세트를 제공합니다. | 2026년 6월 30일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 AI 보안 모범 사례 표준에 대한 8가지 새로운 제어를 릴리스했습니다. 새로운 컨트롤은 Bedrock.1, BedrockAgentCore.7, SageMaker.20, SageMaker.21, SageMaker.22, SageMaker.23, SageMaker.24 및 SageMaker.25입니다. | 2026년 6월 30일 |
| 노출 조사 결과에 대한 영향 특성 유형 및 심각도 업데이트 | 노출 결과에 영향 특성 유형을 추가했습니다. 영향은 연결된 AWS Identity and Access Management 보안 주체의 유효 권한을 기반으로 리소스가 손상된 경우의 잠재적 블래스트 반경을 설명합니다. NIST 지침에 따라 가능성 및 영향 위험 매트릭스를 사용하도록 심각도 계산을 업데이트했습니다. 영향 액세스 경로 특성에 대한 리소스별 문제 해결 지침이 추가되었습니다. | 2026년 6월 23일 |
| 보안 표준 및 제어 업데이트 | ECS.1 및 RDS.18 제어를 사용 중지하고 적용 가능한 모든 표준에서 제거했습니다. Amazon EC2-Classic 네트워킹이 사용 중지되었으므로 Amazon Relational Database Service(Amazon RDS) 인스턴스는 더 이상 VPC 외부에 배포할 수 없습니다. | 2026년 6월 5일 |

| | | |
|---|---|---|
| CSPM 서비스 연결 레코더 업데이트 | Security Hub CSPM이 리소스 구성 정보를 기반으로 보안 제어 검사를 수행할 수 있도록 하는 새로운 서비스 연결 구성 레코더와 관련된 정보가 추가되었습니다. | 2026년 5월 27일 |
| 미사용 액세스 조사 결과 | Security Hub에서 IAM Access Analyzer에서 미사용 액세스 조사 결과를 생성하고 표시하는 기능 추가 Security Hub에서 미사용 액세스 조사 결과 이해 | 2026년 5월 19일 |
| 새로운 보안 제어 | Security Hub CSPM은 다섯 가지 새로운 제어를 릴리스했습니다. 일부 제어는 AWS 기본 보안 모범 사례(FSBP) 표준을 지원합니다. 대부분의 제어는 NIST SP 800-53 개정 5 요구 사항을 지원합니다.<br>• AWS FSBP 표준의 경우 해당 컨트롤IDs는 BedrockAgentCore.5 및 BedrockAgentCore.6입니다.<br>• NIST SP 800-53 개정 5의 경우 해당 컨트롤IDs는 BedrockAgentCore.3, BedrockAgentCore.4 및 SageMaker.18입니다. | 2026년 5월 15일 |

| | | |
|---|---|---|
| 관리형 정책 업데이트 - AWSSecurityHubServiceRolePolicy | Security Hub CSPM은 라는 AWS 관리형 정책을 업데이트했습니다AWSSecurityHubServiceRolePolicy . 업데이트에 Security Hub CSPM 서비스 연결 구성 레코더를 관리하고 AWS Config 서비스 연결 역할을 생성할 수 있는 권한이 추가되었습니다. | 2026년 4월 29일 |
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에 대한 네 가지 새로운 제어를 릴리스했습니다. 새로운 컨트롤은 BedrockAgentCore.1, BedrockAgentCore.2, RDS.51 및 SageMaker.19입니다. | 2026년 4월 22일 |
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에 대한 다섯 가지 새로운 제어를 릴리스했습니다. 새로운 컨트롤은 APIGateway.11, EC2.183, EKS.9, SageMaker.16 및 SageMaker.17입니다. | 2026년 4월 7일 |
| 보안 표준 및 제어 업데이트 | AppSync.1 및 AppSync.6 컨트롤을 사용 중지하고 AWS FSBP(기본 보안 모범 사례) 표준에서 제거했습니다.는 AWS AppSync 이제 모든 현재 및 향후 API 캐시에서 기본 암호화를 제공합니다. | 2026년 3월 9일 |

| | | |
|---|---|---|
| 보안 표준 및 제어 업데이트 | ECS.1 제어를 사용 중지하고 AWS 기본 보안 모범 사례(FSBP) 표준 및 NIST SP 800-53 개정 5 표준에서 제어를 제거했습니다. | 2026년 3월 4일 |
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에 대한 11개의 새로운 제어를 릴리스했습니다. 새로운 컨트롤은 APIGateway.10, ELB.21, ELB.22, RDS.50, SageMaker.9 SageMaker.10 SageMaker.11 SageMaker.12 SageMaker.13 SageMaker.14 및 SageMaker.15입니다. | 2026년 2월 16일 |
| 보안 표준 및 제어 업데이트 | MQ.3 제어를 사용 중지하고 적용 가능한 모든 표준에서 제어를 제거했습니다. 자동 마이너 버전 업그레이드에 대한 Amazon MQ 요구 사항으로 인해 제어가 사용 중지되었습니다.<br><br>이전에는이 제어가 AWS FSBP(기본 보안 모범 사례) 표준, NIST SP 800-53 개정 5 표준 및 PCI DSS v4.0.1 표준에 적용되었습니다. | 2026년 1월 12일 |
| 비용 예측기 설명서 업데이트 | Security Hub 비용 예측기 설명서에 관리 계정 이외의 계정에서 추정을 수행할 수 있는 교차 계정 액세스 권한을 부여하는 방법에 대한 세부 정보가 추가되었습니다. | 2026년 1월 12일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에 대한 다섯 가지 새로운 제어를 릴리스했습니다. 새로운 제어는:CloudFormation.4, CloudFront.17, ECS.19, ECS.20 및 ECS.21입니다. | 2026년 1월 6일 |
| 보안 표준 및 제어 업데이트 | 자동 마이너 버전 업그레이드에 대한 Amazon MQ 요구 사항으로 인해 2026년 1월 12일에 MQ.3을 사용 중지하고 모든 해당 표준에서 제어를 제거할 계획입니다. 현재 제어는 AWS 기본 보안 모범 사례(FSBP) 표준, NIST SP 800-53 개정 5 표준 및 PCI DSS v4.0.1 표준에 적용됩니다. | 2025년 12월 12일 |
| 서비스 관리형 표준의 업데이트된 콘텐츠: AWS Control Tower | 표준에서 제어를 생성, 보기 및 비활성화하기 위한 향상된 지침을 제공하기 위해 서비스 관리형 AWS Control Tower 표준의 콘텐츠가 업데이트되었습니다 AWS Control Tower. | 2025년 12월 8일 |
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에 대한 7가지 새로운 제어를 릴리스했습니다. 새로운 컨트롤은 Cognito.4, Cognito.5, Cognito.6, EC2.182, CloudFormation.3, ECS.18 및 SES.3입니다. | 2025년 12월 8일 |

| | | |
|---|---|---|
| Security Hub 일반 가용성에 대한 업데이트된 콘텐츠 | AWS Security Hub의 일반 가용성 릴리스를 지원하는 콘텐츠 추가 | 2025년 12월 2일 |
| Security Hub의 업데이트된 콘텐츠 | 추세 및 리전 집계에 대한 콘텐츠가 추가되었습니다. 이러한 변경 사항은 Security Hub 미리 보기 릴리스를 지원합니다. | 2025년 11월 21일 |
| 관리형 정책 업데이트 - AWSSecurityHubV2ServiceRolePolicy | Security Hub는 라는 AWS 관리형 정책을 업데이트했습니다AWSSecurityHubV2ServiceRolePolicy . 이 업데이트에는 Security Hub 기능을 지원하기 위해 Amazon Elastic Container Registry AWS Lambda, Amazon CloudWatch 및 AWS Identity and Access Management 에 대한 측정 기능이 추가되었습니다. 이 업데이트에는 글로벌 AWS Config 레코더에 대한 지원도 추가되었습니다. 이러한 변경 사항은 Security Hub 미리 보기 릴리스를 지원합니다. | 2025년 11월 17일 |
| 관리형 정책 업데이트 - AWSSecurityHubOrganizationsAccess | Security Hub는 라는 AWS 관리형 정책을 업데이트했습니다AWSSecurityHubOrganizationsAccess . 이 업데이트에는 Security Hub 기능을 지원하는 리소스 정책을 설명하는 권한이 추가되었습니다. 이러한 변경 사항은 Security Hub 미리 보기 릴리스를 지원합니다. | 2025년 11월 17일 |

| | | |
|---|---|---|
| 관리형 정책 업데이트 - AWSSecurityHubFullAccess | Security Hub는 라는 AWS 관리형 정책을 업데이트했습니다AWSSecurityHubFullAccess . 이 업데이트는 Security Hub 기능을 지원하기 위해 GuardDuty, Amazon Inspector 및 계정 관리에 대한 기능을 추가했습니다. 이러한 변경 사항은 Security Hub 미리 보기 릴리스를 지원합니다. | 2025년 11월 17일 |
| 보안 제어 업데이트 | CloudFront.7, CloudTrail.5, ELB.7, GuardDuty.7, MQ.3, Opensearch.10, RDS.7, ServiceCatalog.1, SNS.4, SQS.3 등 10가지 Security Hub CSPM 제어의 심각도를 변경했습니다. 변경 사항에 대한 자세한 내용은 Security Hub CSPM 제어에 대한 변경 로그를 참조하세요. | 2025년 11월 13일 |
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에 대한 6가지 새로운 제어를 릴리스했습니다. 새로운 제어는 Cognito.3, DMS.13, EC2.181, RDS.43, RDS.47, RDS.48입니다. | 2025년 10월 28일 |

| | | |
|---|---|---|
| 새로운 보안 표준 | Security Hub CSPM은 이제 CIS AWS Foundations Benchmark v5.0.0에 맞는 보안 표준을 제공합니다. 이 새로운 표준에는 40개의 기존 보안 제어가 포함되어 있습니다. 제어는 특정 리소스가 이 프레임워크에 정의된 요구 사항의 하위 집합을 준수하는지 평가하는 자동 검사를 수행합니다. | 2025년 10월 16일 |
| 새로운 서드 파티 통합 | Elastic은 Security Hub CSPM에서 조사 결과를 수신할 수 있는 서드 파티 통합입니다. | 2025년 10월 3일 |
| 보안 표준 및 제어 업데이트 | Redshift.9 및 RedshiftServerless.7 제어를 사용 중지하고 모든 적용 가능한 표준에서 제거했습니다. 이러한 제어에 대한 FAILED 조사 결과를 효과적으로 해결할 수 없었던 Amazon Redshift에 내재된 제한으로 인해 해당 제어를 중지했습니다.<br><br>이전에는 이러한 제어가 AWS 기본 보안 모범 사례(FSBP) 표준 및 NIST SP 800-53 개정 5 표준에 적용되었습니다. Redshift.9 제어는 AWS Control Tower 서비스 관리형 표준에도 적용되었습니다. | 2025년 9월 24일 |

| | | |
|---|---|---|
| 리전별 가용성 | 이제 아시아 태평양(뉴질랜드) 리전에서 Security Hub CSPM을 사용할 수 있습니다. Security Hub CSPM을 현재 사용할 수 AWS 리전 있는 전체 목록은의 AWS Security Hub 엔드포인트 및 할당량을 참조하세요AWS 일반 참조. | 2025년 9월 19일 |
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에 대한 2개의 새로운 제어 CloudFront.16 및 RDS.46을 릴리스했습니다. | 2025년 9월 3일 |
| 리전별 가용성 | 이제 아시아 태평양(태국) 및 멕시코(중부) 리전에서 AWS 리소스 태그 지정 표준을 사용할 수 있습니다. | 2025년 8월 29일 |
| 보안 표준 및 제어 업데이트 | Amazon Redshift 제한 사항으로 인해 2025년 9월 15일에 Redshift.9 및 RedshiftServerless.7 제어를 사용 중지하고 모든 적용 가능한 표준에서 제거할 계획입니다. 현재, 이러한 제어는 AWS FSBP(기본 보안 모범 사례) 표준 및 NIST SP 800-53 개정 5 표준에 적용됩니다. Redshift.9 제어는 AWS Control Tower 서비스 관리형 표준에도 적용됩니다. | 2025년 8월 15일 |

| | | |
|---|---|---|
| ASFF의 새로운 리소스 세부 정보 객체 | 이제 AWS Security Finding Format(ASFF)에 CodeRepository 리소스 객체가 포함됩니다. 이 객체는 AWS 리소스에 연결하고 취약성을 검사하도록 Amazon Inspector를 구성한 외부 코드 리포지토리에 대한 세부 정보를 제공합니다. | 2025년 8월 1일 |
| 리전별 가용성 | 이제 아시아 태평양(타이베이) 리전에서 Security Hub CSPM을 사용할 수 있습니다. 현재 Security Hub CSPM을 사용할 수 있는 AWS 리전 의 목록은 AWS 일반 참조의 AWS Security Hub CSPM 엔드포인트 및 할당량을 참조하세요. | 2025년 7월 23일 |
| 새로운 서드 파티 통합 | Dynatrace은 Security Hub CSPM에서 조사 결과를 수신할 수 있는 서드 파티 통합입니다. | 2025년 7월 18일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 13개의 새로운 제어를 릴리스했습니다. 대부분의 제어는 AWS 기본 보안 모범 사례(FSBP) 표준을 지원합니다. 일부 제어는 NIST SP 800-53 개정 5 요구 사항을 지원합니다.<br>• AWS FSBP 표준의 경우 해당 컨트롤의 IDs는 CloudFront.15, Cognito.2, EC2.180, ELB.18, MSK.4, MSK.5, MSK.6, RDS.45, Redshift.18, S3.25, SSM.6 및 SSM.7입니다.<br>• NIST SP 800-53 개정 5의 경우 해당 제어의 ID는 Lambda.7 및 RDS.45입니다. | 2025년 7월 15일 |
| 제어 조사 결과 생성 업데이트 | 규정 준수 변경 사항을 추적하는 데 도움이 되도록 Security Hub CSPM은 이제 개별 리소스의 규정 준수 상태가 변경될 때 새 조사 결과를 생성하는 대신 기존 제어 조사 결과를 업데이트합니다. 즉, 개별 조사 결과에서 제공하는 데이터를 사용하여 특정 리소스의 특정 제어에 대한 규정 준수 변경을 추적할 수 있습니다. | 2025년 7월 3일 |

| | | |
|---|---|---|
| 보안 표준 및 제어 업데이트 | PCI DSS v4.0.1 표준에서 IAM.13 제어를 제거했습니다. 또한 NIST SP 800-171 개정 2 표준에서 IAM.17 제어를 제거했습니다. 표준은 이러한 제어가 제공하는 검사를 명시적으로 요구하지 않습니다. 또한 IAM 암호 정책을 확인하는 제어인 IAM.7 및 IAM.10~IAM.17에 대한 이러한 표준의 관련 요구 사항 세부 정보를 업데이트했습니다. | 2025년 6월 30일 |
| 조사 결과 보존 업데이트 | Security Hub CSPM은 이제 보관된 결과를 90일이 아닌 30일 동안 저장하므로 조사 결과 노이즈를 줄일 수 있습니다. 장기 보존을 위해, Amazon EventBridge 규칙과 함께 사용자 지정 작업을 사용하여 조사 결과를 S3 버킷으로 내보낼 수 있습니다. | 2025년 6월 20일 |

| | | |
|---|---|---|
| 기존 관리형 정책 업데이트 | Security Hub CSPM은 AWS 관리형 정책에 `AWSSecurityHubOrganizationsAccess` 라는 새 권한을 추가했습니다. 이 권한을 통해 조직 관리는 조직 내에서 Security Hub 및 Security Hub CSPM을 활성화하고 관리할 수 있습니다. 또한 Security Hub CSPM은 AWS 관리형 정책에 `AWSSecurityHubFullAccess` 라는 새 권한을 추가했습니다. 이러한 권한을 사용하여 위탁자는 Security Hub용 서비스 연결 역할을 생성할 수 있습니다. | 2025년 6월 18일 |
| Security Hub의 공개 프리뷰 릴리스 및 새로운 관리형 정책 | AWS Security Hub의 공개 평가판 릴리스 및 AWS Security Hub 사용 설명서. 이 릴리스에는 새로운 AWS 관리형 정책인 `AWSSecurityHubV2ServiceRolePolicy` 가 포함되어 있습니다. 이 정책은 Security Hub가 고객의 조직에서 고객을 대신하여 AWS Config 규칙과 Security Hub 리소스를 관리할 수 있도록 허용합니다. Security Hub는 현재 프리뷰 버전이 출시 중이기 때문에 변경될 수도 있습니다. | 2025년 6월 17일 |

| | | |
|---|---|---|
| 보안 표준 및 제어 업데이트 | PCI DSS v4.0.1 표준에서 IAM.10 제어를 제거했습니다. 이 제어는 IAM 사용자의 계정 암호 정책이 최소 암호 길이 7자를 포함한 최소 요구 사항을 충족하는지 확인합니다. PCI DSS v4.0.1은 이제 최소 암호 길이로 8자를 요구합니다. 암호 요구 사항이 다른 PCI DSS v3.2.1 표준에는 IAM.10 제어가 계속 적용됩니다. | 2025년 5월 30일 |
| 새로운 보안 표준 | Security Hub CSPM은 이제 NIST SP 800-171 개정 2 사이버 보안 및 규정 준수 프레임워크에 부합하는 보안 표준을 제공합니다. 이 새로운 표준에는 60개 이상의 기존 보안 제어가 포함되어 있습니다. 제어는 프레임워크에서 정의한 요구 사항의 하위 집합을 준수하는지 특정 AWS 서비스 및 리소스를 평가하는 자동 검사를 수행합니다. | 2025년 5월 29일 |
| 보안 제어 업데이트 | Security Hub CSPM은 모든에서 다음 제어의 릴리스를 롤백했습니다. AWS 리전[RDS.46] RDS DB 인스턴스는 인터넷 게이트웨이에 대한 경로가 있는 퍼블릭 서브넷에 배포해서는 안 됩니다. 이전에는이 제어가 AWS 기본 보안 모범 사례(FSBP) 표준을 지원했습니다. | 2025년 5월 8일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 9개의 새로운 제어를 릴리스했습니다. 대부분의 제어는 AWS 기본 보안 모범 사례(FSBP) 표준을 지원합니다. 일부 제어는 NIST SP 800-53 개정 5 요구 사항을 지원합니다.<br>• AWS FSBP 표준의 경우 해당 컨트롤의 IDs는 DocumentDB.6, RDS.44, RedshiftServerless.2, RedshiftServerless.3, RedshiftServerless.5, RedshiftServerless.6 및 RedshiftServerless.7(나중에 사용 중지됨)입니다.<br>• NIST SP 800-53 개정 5의 경우 해당 제어의 ID는 다음과 같습니다. CloudTrail.10, RedshiftServerless.4, RedshiftServerless.7(나중에 사용 중지됨). | 2025년 5월 7일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 24개의 새로운 제어를 릴리스했습니다. 대부분의 제어는 AWS 기본 보안 모범 사례(FSBP) 또는 AWS 리소스 태그 지정 표준을 지원합니다. 일부 제어는 NIST SP 800-53 개정 5 요구 사항을 지원합니다.<br>• AWS FSBP 표준의 경우 해당 컨트롤IDs는 EC2.173, RDS.41, RDS.42 및 SageMaker.8입니다.<br>• AWS 리소스 태그 지정 표준의 경우 해당 컨트롤의 IDs는 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 및 Transfer.7입니다.<br>• NIST SP 800-53 개정 5의 경우 해당 제어의 ID는 ECS.17 및 RDS.42입니다. | 2025년 4월 16일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 AWS 기본 보안 모범 사례 표준을 지원하는 4개의 새로운 제어를 릴리스했습니다. 제어는 다음과 같습니다.<br>• the section called “[FSx.3] FSx for OpenZFS 파일 시스템에는 다중 AZ 배포를 구성해야 합니다.”<br>• the section called “[FSx.4] FSx for NetApp ONTAP 파일 시스템에는 다중 AZ 배포를 구성해야 합니다”<br>• the section called “[FSx.5] FSx for Windows File Server 파일 시스템에는 다중 AZ 배포를 구성해야 합니다”<br>• the section called “[RedshiftServerless.1] Amazon Redshift Serverless 작업 그룹은 향상된 VPC 라우팅을 사용해야 합니다” | 2025년 3월 18일 |
| 보안 표준 및 제어 업데이트 | AWS 기본 보안 모범 사례 표준 및 NIST SP 800-53 개정 5 요구 사항에 대한 자동 검사에서 RDS.18 보안 제어(나중에 사용 중지됨)를 제거했습니다. Amazon EC2-Classic 네트워킹이 사용 중지되었으므로 Amazon Relational Database Service(Amazon RDS) 인스턴스는 더 이상 VPC 외부에 배포할 수 없습니다. | 2025년 3월 7일 |

| | | |
|---|---|---|
| 제어 조사 결과 업데이트 | 이제 Security Hub CSPM은 제어가 확인하는 리소스 유형에 대해 리소스 기록이에서 활성화되지 않은 경우 활성화된 제어에 AWS Config 대한 WARNING 조사 결과를 생성합니다. 이를 통해 보안 제어 검사의 잠재적 구성 격차를 식별하고 해결할 수 있습니다. | 2025년 2월 25일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 11개의 새로운 제어를 릴리스했습니다. 제어는 다음과 같습니다.<br>• the section called “[Connect.2] 고객 인스턴스 연결에는 CloudWatch 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[ECR.5] ECR 리포지토리는 고객 관리형 로 암호화해야 합니다. AWS KMS keys”<br>• the section called “[ELB.17] 리스너가 있는 Application Load Balancer 및 Network Load Balancer는 권장 보안 정책을 사용해야 합니다”<br>• the section called “[Glue.4] AWS Glue스파크 작업은의 지원되는 버전에서 실행되어야 합니다.AWS Glue”<br>• the section called “[GuardDuty.11] GuardDuty 런타임 모니터링을 활성화해야 합니다”<br>• the section called “[GuardDuty.12] GuardDuty ECS Runtime Monitoring이 활성화되어 있어야 합니다”<br>• the section called “[GuardDuty.13] GuardDuty EC2 런타임 모니터링을 활성화해야 합니다”<br>• the section called “[Network Firewall.10] Network | 2025년 2월 24일 |

| | | |
|---|---|---|
| | Firewall 방화벽에는 서브넷 변경 방지가 활성화되어 있어야 합니다”<br>• the section called “[RDS.40] RDS for SQL Server DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다”<br>• the section called “[SQS.3] SQS 대기열 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다”<br>• the section called “[Transfer.3] Transfer Family 커넥터에는 로깅이 활성화되어 있어야 합니다” | |
| 새로운 보안 제어 | Security Hub CSPM은 AWS 리소스 태그 지정 표준을 지원하는 37개의 새로운 제어를 릴리스했습니다. Security Hub CSPM은 다음과 같은 새로운 제어도 릴리스했습니다.<br>• the section called “[EMR.3] Amazon EMR 보안 구성은 저장 시 암호화되어야 합니다”<br>• the section called “[EMR.4] Amazon EMR 보안 구성은 전송 중 암호화되어야 합니다”<br>• the section called “[SageMaker.5] SageMaker 모델에는 네트워크 격리가 활성화되어 있어야 합니다” | 2025년 1월 22일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | Security Hub CSPM은 EC2.172 EC2 VPC 퍼블릭 액세스 차단 설정이 인터넷 게이트웨이 트래픽을 차단해야 합니다를 릴리스했습니다. | 2025년 1월 15일 |
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[Cognito.1] Cognito 사용자 풀에는 표준 인증을 위한 전체 기능 적용 모드로 위협 방지가 활성화되어 있어야 합니다”<br>• the section called “[RDS.38] RDS for PostgreSQL DB 인스턴스는 전송 중 암호화되어야 합니다”<br>• the section called “[RDS.39] RDS for MySQL DB 인스턴스는 전송 중 암호화되어야 합니다”<br>• the section called “[Redshift.16] Redshift 클러스터 서브넷 그룹에는 여러 가용 영역의 서브넷이 있어야 합니다” | 2024년 12월 17일 |
| Security Hub CSPM이 PCI DSS v4.0.1을 지원 | Security Hub CSPM은 이제 PCI DSS(지불 카드 산업 데이터 보안 표준) v4.0.1을 지원합니다. 해당 표준 및 적용되는 제어에 대한 자세한 내용은 Security Hub CSPM의 PCI DSS를 참조하세요. | 2024년 12월 11일 |

| | | |
|---|---|---|
| Security Hub CSPM이 GuardDuty 공격 시퀀스 조사 결과를 수신 | Security Hub CSPM은 이제 Amazon GuardDuty Extended Threat Detection으로부터 공격 시퀀스 조사 결과를 수신합니다. 공격 시퀀스 결과 세부 정보는 AWS Security Finding Format(ASFF)의 Detection 객체에서 확인할 수 있습니다. | 2024년 12월 1일 |
| 새로운에서 지원되는 Security Hub CSPM AWS 리전 | 이제 아시아 태평양(말레이시아) 리전에서 Security Hub CSPM을 사용할 수 있습니다. 일부 보안 제어에는 리전 제한이 있습니다. 이 리전에서 사용할 수 없는 제어의 목록은 Security Hub CSPM 제어에 대한 리전 제한을 참조하세요. | 2024년 11월 22일 |
| Config.1 변경 사항 | Security Hub CSPM은 Config.1 제어의 심각도를 `MEDIUM`에서 `CRITICAL`로 상향하고 Config.1 실패 결과에 대한 새로운 상태 코드 및 상태 사유를 추가했습니다. 변경 사항에 대한 자세한 내용은 Security Hub CSPM 제어의 변경 로그에서 2024년 11월 20일 항목을 참조하세요. | 2024년 11월 20일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다. 이러한 제어는 AWS 기본 보안 모범 사례 및 NIST SP 800-53 개정 5의 일부이며 관리하는 Virtual Private Cloud(VPC)에 AWS 서비스 또는 AWS 리소스에 대한 인터페이스 VPC 엔드포인트가 있는지 평가합니다.<br>• the section called “[EC2.55] VPC는 ECR API용 인터페이스 엔드포인트로 구성해야 합니다”<br>• the section called “[EC2.56] VPC는 Docker Registry용 인터페이스 엔드포인트로 구성해야 합니다”<br>• the section called “[EC2.57] VPC는 Systems Manager용 인터페이스 엔드포인트로 구성해야 합니다”<br>• the section called “[EC2.58] VPC는 Systems Manager Incident Manager Contacts용 인터페이스 엔드포인트로 구성해야 합니다”<br>• the section called “[EC2.60] VPC는 Systems Manager Incident Manager용 인터페이스 엔드포인트로 구성해야 합니다” | 2024년 11월 15일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[AppSync.1]AWS AppSyncAPI 캐시는 저장 시 암호화되어야 합니다.”<br>• the section called “[AppSync.6]AWS AppSyncAPI 캐시는 전송 중에 암호화되어야 합니다.”<br>• the section called “[EC2.170] EC2 런치 템플릿은 인스턴스 메타데이터 서비스 버전 2(IMDSv2)를 사용해야 합니다.”<br>• the section called “[EC2.171] EC2 VPN 연결에는 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[EFS .8] EFS 파일 시스템은 저장 시 암호화해야 합니다.”<br>• the section called “[KMS.5] KMS 키는 공개적으로 액세스할 수 없어야 합니다.”<br>• the section called “[SNS.4] SNS 주제 액세스 정책은 퍼블릭 액세스를 허용해서는 안 됩니다.” | 2024년 10월 18일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[ECS.16] ECS 작업 세트는 퍼블릭 IP 주소를 자동으로 할당해서는 안 됩니다.”<br>• the section called “[GuardDuty.7] GuardDuty EKS 런타임 모니터링을 활성화해야 합니다.”<br>• the section called “[Kinesis.3] Kinesis 스트림에는 적절한 데이터 보존 기간이 있어야 합니다.”<br>• the section called “[MSK.3] MSK Connect 커넥터는 전송 중에 암호화되어야 합니다.”<br>• the section called “[RDS.36] RDS for PostgreSQL DB 인스턴스는 로그를 CloudWatch Logs에 게시해야 합니다.”<br>• the section called “[RDS.37] Aurora MySQL DB 클러스터는 CloudWatch Logs에 로그를 게시해야 합니다.”<br>• the section called “[S3.24] S3 다중 리전 액세스 포인트에 공개 액세스 차단 설정이 활성화되어 있어야 합니다” | 2024년 10월 3일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[Athena.4] Athena 작업 그룹에 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[CodeBuild.7] CodeBuild 보고서 그룹 내보내기는 저장 시 암호화되어야 합니다.”<br>• the section called “[DataSync.1] DataSync 작업에는 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[EFS .7] EFS 파일 시스템에는 자동 백업이 활성화되어 있어야 합니다.”<br>• Glue.2(사용 중지됨)<br>• the section called “[Glue.3] AWS Glue기계 학습 변환은 저장 시 암호화되어야 합니다.”<br>• the section called “[WorkSpaces.1] WorkSpaces 사용자 볼륨은 저장 시 암호화해야 합니다.”<br>• the section called “[WorkSpaces.2] WorkSpaces 루트 볼륨은 저장 시 암호화해야 합니다.” | 2024년 8월 30일 |

| | | |
|---|---|---|
| 새로운 조사 결과 패널 | Security Hub CSPM 콘솔의 새로운 조사 결과 패널은 조사 결과에 대한 조치를 신속하게 취하고, 리소스 세부 정보 및 조사 결과 기록을 검토하고, 조사 결과에 대한 기타 관련 정보를 찾는 데 도움이 됩니다. | 2024년 8월 16일 |
| Config.1 제어 업데이트 | Config.1 제어는 AWS Config 가 활성화되었는지 확인하고, 서비스 연결 역할을 사용하고, 활성화된 제어에 대한 리소스를 기록합니다. Security Hub CSPM은 `includeConfigServiceLinkedRoleCheck` 라는 사용자 지정 제어 파라미터를 추가했습니다. 이 파라미터를 `false`(으)로 설정하면 AWS Config 이(가) 서비스 연결 역할을 사용하는지 여부를 확인하지 않도록 선택할 수 있습니다. | 2024년 8월 15일 |
| 연결된 리전이 없는 홈 리전 지정 | 이제 홈 리전에 연결하지 않고도 조사 결과 집계자를 생성하고 홈 리전 AWS 리전 을 설정할 수 있습니다. 이렇게 하면 연결된 리전을 지정하지 않고도 중앙 구성을 활성화할 수 있습니다. | 2024년 7월 25일 |

| | | |
|---|---|---|
| 더 많은 리전에서 사용 가능한 제어 선택 | 이제 미국 동부(버지니아 북부) 및 미국 동부(오하이오)를 AWS 리전포함한 추가에서 다음 제어를 사용할 수 있습니다.<br>• the section called “[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.”<br>• the section called “[DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.”<br>• the section called “[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.”<br>• the section called “[DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.”<br>• the section called “[DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다”<br>• the section called “[EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다”<br>• the section called “[EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.” | 2024년 7월 15일 |

- the section called “[FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.”
- the section called “[MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.”
- [MQ.3] Amazon MQ 브로커에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- the section called “[Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.”
- the section called “[Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.”
- the section called “[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.”
- the section called “[ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.”
- the section called “[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.”

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[GuardDuty.5] GuardDuty EKS 감사 로그 모니터링을 활성화해야 합니다.”<br>• the section called “[GuardDuty.6] GuardDuty Lambda 보호를 활성화해야 합니다.”<br>• the section called “[GuardDuty.8] EC2에 대한 GuardDuty 맬웨어 보호가 활성화되어야 합니다.”<br>• the section called “[GuardDuty.9] GuardDuty RDS 보호를 활성화해야 합니다.”<br>• the section called “[GuardDuty.10] GuardDuty S3 보호를 활성화해야 합니다.”<br>• the section called “[Inspector.1] Amazon Inspector EC2 스캔을 활성화해야 합니다.”<br>• the section called “[Inspector.2] Amazon Inspector ECR 스캔을 활성화해야 합니다.”<br>• the section called “[Inspector.3] Amazon Inspector Lambda 코드 스캔을 활성화해야 합니다.”<br>• the section called “[Inspector.4] Amazon Inspector Lambda 표준 스캔을 활성화해야 합니다.” | 2024년 7월 11일 |

| | | |
|---|---|---|
| CIS AWS 파운데이션 벤치마크 v3.0.0 릴리스 | Security Hub CSPM에서 Center for Internet Security(CIS) AWS Foundations Benchmark v3.0.0을 릴리스했습니다. 이 릴리스에는 다음과 같은 새로운 제어와 여러 기존 제어에 대한 매핑이 포함되어 있습니다.<br>• the section called “[EC2.53] EC2 보안 그룹은 0.0.0.0/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다”<br>• the section called “[EC2.54] EC2 보안 그룹은 ::/0에서 원격 서버 관리 포트로의 수신을 허용하지 않아야 합니다”<br>• the section called “[IAM.26] IAM에서 관리되는 만료된 SSL/TLS 인증서를 제거해야 합니다.”<br>• the section called “[IAM.27] IAM 자격 증명에는 AWSCloudShellFullAccess 정책이 연결되지 않아야 합니다.”<br>• the section called “[IAM.28] IAM Access Analyzer 외부 액세스 분석기를 활성화해야 합니다.”<br>• the section called “[S3.22] S3 범용 버킷은 객체 수준 쓰기 이벤트를 기록해야 합니다.” | 2024년 5월 13일 |

- the section called “[S3.23] S3 범용 버킷은 객체 수준 읽기 이벤트를 기록해야 합니다.”

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[DataFirehose.1] Firehose 전송 스트림은 저장 시 암호화해야 합니다.”<br>• the section called “[DMS.10] Neptune 데이터베이스용 DMS 엔드포인트에는 IAM 인증이 활성화되어 있어야 합니다.”<br>• the section called “[DMS.11] MongoDB용 DMS 엔드포인트에는 인증 메커니즘이 활성화되어 있어야 합니다.”<br>• the section called “[DMS.12] Redis OSS용 DMS 엔드포인트에는 TLS가 활성화되어 있어야 합니다.”<br>• the section called “[DynamoDB.7] DynamoDB Accelerator 클러스터는 전송 중에 암호화되어야 합니다”<br>• the section called “[EFS.6] EFS 탑재 대상은 시작 시 퍼블릭 IP 주소를 할당하는 서브넷과 연결되어서는 안 됩니다”<br>• the section called “[EKS.3] EKS 클러스터는 암호화된 Kubernetes 보안 암호를 사용해야 합니다.” | 2024년 5월 3일 |

- the section called “[FSx.2] FSx for Lustre 파일 시스템이 백업에 태그를 복사하도록 구성되어 있어야 합니다.”
- the section called “[MQ.2] ActiveMQ 브로커는 감사 로그를 CloudWatch로 스트리밍해야 합니다.”
- [MQ.3] Amazon MQ 브로커에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.
- the section called “[Opensearch.11] OpenSearch 도메인에는 최소 3개의 전용 프라이머리 노드가 있어야 합니다.”
- the section called “[Redshift.15] Redshift 보안 그룹은 제한된 오리진에서만 클러스터 포트의 수신을 허용해야 합니다.”
- the section called “[SageMaker.4] SageMaker 엔드포인트 프로덕션 변형의 초기 인스턴스 수는 1보다 커야 합니다.”
- the section called “[ServiceCatalog.1] Service Catalog 포트폴리오는 AWS조직 내에서만 공유해야 합니다.”
- the section called “[Transfer.2] Transfer Family 서버는 엔드포인트 연결에 FTP 프로토콜을 사용해서는 안 됩니다.”

| | | |
|---|---|---|
| AWS 리소스 태그 지정 표준 | 이제 Security Hub CSPM의 AWS 리소스 태그 지정 표준과 표준에 적용되는 새로운 제어 기능을 일반적으로 사용할 수 있습니다. | 2024년 4월 30일 |
| 기존 관리형 정책 업데이트 | Security Hub CSPM은 AWS 서비스 및 제품에 대한 요금 세부 정보를 얻`AmazonSecurityHubFullAccess` 기 위해 라는 AWS 관리형 정책을 업데이트했습니다. | 2024년 4월 24일 |
| 제어 파라미터의 컨텍스트 내 구성 | 중앙 구성을 사용하는 경우, 이제 Security Hub CSPM 콘솔의 제어에 있는 세부 정보 페이지로부터 컨텍스트 내의 제어 파라미터를 구성할 수 있습니다. | 2024년 3월 29일 |
| 기존 관리형 정책 업데이트 | Security Hub CSPM은 `Sid` 필드를 추가하여 `AWSSecurityHubReadOnlyAccess` 이라는 이름의 AWS 관리형 정책을 업데이트했습니다. | 2024년 2월 22일 |
| 새로운 보안 제어 | 이제 제어 [Macie.2] Macie의 민감한 데이터 자동 검색을 활성화해야 합니다를 사용할 수 있습니다. 이 제어에 대한 리전별 제한은 리전별 제어 가용성을 참조하세요. | 2024년 2월 19일 |

| | | |
|---|---|---|
| Security Hub CSPM을 캐나다 서부(캘거리)에서 사용 가능 | 이제 캐나다 서부(캘거리)에서 Security Hub CSPM을 사용할 수 있습니다. 이제 특정 보안 제어를 제외한 모든 Security Hub CSPM 기능을 이 리전에서 사용할 수 있습니다. 자세한 내용은 리전별 제어 가용성을 참조하세요. | 2023년 12월 20일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[Backup.1]AWS Backup복구 지점은 저장 시 암호화되어야 합니다.”<br>• the section called “[DynamoDB.6] DynamoDB 테이블에는 삭제 방지 기능이 활성화되어 있어야 합니다.”<br>• the section called “[EC2.51] EC2 Client VPN 엔드포인트에는 클라이언트 연결 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[EKS.8] EKS 클러스터에는 감사 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[EMR.2] Amazon EMR 퍼블릭 액세스 차단 설정을 활성화해야 합니다.”<br>• the section called “[FSx.1] FSx for OpenZFS 파일 시스템이 백업 및 볼륨에 태그를 복사하도록 구성되어 있어야 합니다.”<br>• the section called “[Macie.1] Amazon Macie가 활성화되어야 합니다.” | 2023년 12월 14일 |

- the section called “[MSK.2] MSK 클러스터에는 향상된 모니터링이 구성되어 있어야 합니다.”
- the section called “[Neptune.9] Neptune DB 클러스터를 여러 가용 영역에 배포해야 합니다.”
- the section called “[Network Firewall.1] Network Firewall 방화벽을 여러 가용 영역에 배포해야 합니다.”
- the section called “[Network Firewall.2] Network Firewall 로깅을 활성화해야 합니다.”
- the section called “[Opensearch.10] OpenSearch 도메인에는 최신 소프트웨어 업데이트가 설치되어 있어야 합니다.”
- the section called “[PCA.1]AWS Private CA루트 인증 기관을 비활성화해야 합니다.”
- the section called “[S3.19] S3 액세스 포인트에 퍼블릭 액세스 차단 설정이 활성화되어 있어야 합니다.”
- the section called “[S3.20] S3 범용 버킷에는 MFA 삭제가 활성화되어 있어야 합니다.”

| | | |
|---|---|---|
| 조사 결과 보강 | Security Hub CSPM은 새로운 결과 필드 `AwsAccountName` , `ApplicationArn` 및를 AWS Security Finding Format(ASFF)`ApplicationName` 에 추가했습니다. | 2023년 11월 27일 |
| 요약 대시보드 개선 사항 | 이제 Security Hub CSPM 콘솔의 요약 페이지에서 더 많은 대시보드 위젯에 액세스하고, 대시보드 필터 세트를 저장하여 특정 보안 문제에 빠르게 집중하고, 대시보드 레이아웃을 사용자 지정할 수 있습니다. | 2023년 11월 27일 |
| 중앙 구성 | 이제 중앙 구성을 사용할 수 있습니다. 중앙 구성을 통해 Security Hub CSPM 위임된 관리자는 여러 조직 계정, 조직 단위(OU) 및 리전에 걸쳐 Security Hub CSPM, 표준 및 제어를 구성할 수 있습니다. | 2023년 11월 27일 |
| 관리형 정책으로 업데이트 | Security Hub CSPM은 Security Hub CSPM이 사용자 지정 가능한 보안 제어 속성을 읽고 업데이트할 수 있는 새로운 권한을 관리형 `AWSSecurityHubServiceRolePolicy` 정책에 추가했습니다. | 2023년 11월 26일 |

| | | |
|---|---|---|
| 사용자 지정 제어 파라미터 | 이제 일부 Security Hub CSPM 제어의 파라미터 값을 사용자 지정할 수 있습니다. 이렇게 하면 특정 제어에 대한 조사 결과를 비즈니스 요구 사항 및 보안 기대치에 더 적합하게 만들 수 있습니다. | 2023년 11월 26일 |
| 관리형 정책으로 업데이트 | Security Hub CSPM은 각각 Security Hub CSPM 기능과 AWS Organizations와의 통합을 사용할 수 있도록 허용하는 `AWSSecurityHubFullAccess` 및 `AWSSecurityHubOrganizationsAccess` 관리형 정책을 업데이트했습니다. | 2023년 11월 16일 |

| | | |
|---|---|---|
| 서비스 관리형 표준에 추가된 기존 보안 제어: AWS Control Tower | 서비스 관리형 표준에 다음과 같은 기존 Security Hub CSPM 제어가 추가되었습니다 AWS Control Tower.<br>• ACM.2<br>• AppSync.5<br>• CloudTrail.6<br>• DMS.9<br>• DocumentDB.3<br>• DynamoDB.3<br>• EC2.23<br>• EKS.1<br>• ElastiCache.3<br>• ElastiCache.4<br>• ElastiCache.5<br>• ElastiCache.6<br>• EventBridge.3<br>• KMS.4<br>• Lambda.3<br>• MQ.5<br>• MQ.6<br>• MSK.1<br>• RDS.12<br>• RDS.15<br>• S3.17 | 2023년 11월 14일 |

| | | |
|---|---|---|
| 관리형 정책으로 업데이트 | Security Hub CSPM은 Security Hub CSPM이 조사 결과와 관련된 리소스 태그를 읽을 수 있도록 하는 새로운 태그 지정 권한을 `AWSSecurityHubServiceRolePolicy` 관리형 정책에 추가했습니다. | 2023년 11월 7일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[AppSync.5]AWS AppSyncGraphQL APIs API 키로 인증해서는 안 됩니다.”<br>• the section called “[DMS.6] DMS 복제 인스턴스에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.”<br>• the section called “[DMS.7] 대상 데이터베이스에 대한 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[DMS.8] 소스 데이터베이스의 DMS 복제 작업에는 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[DMS.9] DMS 엔드포인트는 SSL을 사용해야 합니다.”<br>• the section called “[DocumentDB.3] Amazon DocumentDB 수동 클러스터 스냅샷은 공개되어서는 안 됩니다.”<br>• the section called “[DocumentDB.4] Amazon DocumentDB 클러스터는 CloudWatch Logs에 감사 로그를 게시해야 합니다.” | 2023년 10월 10일 |

- the section called “[DocumentDB.5] Amazon DocumentDB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.”
- the section called “[ECS.9] ECS 작업 정의에는 로깅 구성이 있어야 합니다.”
- the section called “[EventBridge.3] EventBridge 사용자 지정 이벤트 버스에는 리소스 기반 정책이 연결되어 있어야 합니다.”
- the section called “[EventBridge.4] EventBridge 글로벌 엔드포인트에는 이벤트 복제가 활성화되어 있어야 합니다.”
- the section called “[MSK.1] MSK 클러스터는 브로커 노드 간 전송 중 암호화되어야 합니다.”
- the section called “[MQ.5] ActiveMQ 브로커는 활성/대기 배포 모드를 사용해야 합니다.”
- the section called “[MQ.6] RabbitMQ 브로커는 클러스터 배포 모드를 사용해야 합니다”
- the section called “[NetworkFirewall.9] 네트워크 방화벽에는 삭제 방지 기능이 활성화되어 있어야 합니다.”

| | | |
|---|---|---|
| | • the section called “[RDS.34] Aurora MySQL DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.”<br>• the section called “[RDS.35] RDS DB 클러스터에는 자동 마이너 버전 업그레이드가 활성화되어 있어야 합니다.”<br>• the section called “[Route53.2] Route53 퍼블릭 호스팅 영역은 DNS 쿼리를 로깅해야 합니다.”<br>• the section called “[WAF.12] AWS WAF규칙에는 CloudWatch 지표가 활성화되어 있어야 합니다.” | |
| 관리형 정책으로 업데이트 | Security Hub CSPM은 Security Hub CSPM이 계정 및 조직 단위(OU) 정보를 검색할 수 있도록 하는 새로운 Organizations 작업을 `AWSSecurityHubServiceRolePolicy` 관리형 정책에 추가했습니다. 또한 Security Hub CSPM이 표준 및 제어를 포함한 서비스 구성을 읽고 업데이트할 수 있도록 하는 새로운 Security Hub CSPM 작업도 추가했습니다. | 2023년 9월 27일 |

| | | |
|---|---|---|
| 서비스 관리형 표준에 추가된 기존 보안 제어: AWS Control Tower | 서비스 관리형 표준에 다음과 같은 기존 Security Hub CSPM 제어가 추가되었습니다 AWS Control Tower.<br>• the section called “[Athena.1] Athena 워크그룹은 저장 시 암호화되어야 합니다”<br>• the section called “[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.”<br>• the section called “[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.”<br>• the section called “[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.”<br>• the section called “[Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.”<br>• the section called “[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.”<br>• the section called “[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.”<br>• the section called “[Neptune.5] Neptune DB 클러스터에 | 2023년 9월 26일 |

| | | |
|---|---|---|
| | 는 자동 백업이 활성화되어 있어야 합니다.”<br>• the section called “[Neptune .6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.”<br>• the section called “[Neptune .7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.”<br>• the section called “[Neptune .8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.”<br>• the section called “[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.” | |
| 에서 사용 가능한 통합 제어 보기 및 통합 제어 결과 AWS GovCloud (US) | 이제 AWS GovCloud (US) Region에서 통합 제어 보기 및 통합 제어 조사 결과를 사용할 수 있습니다. Security Hub CSPM 콘솔의 제어 페이지에는 표준 전체의 모든 제어가 표시됩니다. 표준 전체에서 각 제어에는 동일한 제어 ID가 있습니다. 통합 제어 조사 결과를 켜면 제어가 활성화된 여러 표준에 적용되는 경우에도 보안 검사당 단일 조사 결과를 받게 됩니다. | 2023년 9월 6일 |

| | | |
|---|---|---|
| 중국 리전에서 통합 제어 보기 및 통합 제어 조사 결과를 사용 가능 | 이제 중국 리전에서 통합 제어 보기 및 통합 제어 조사 결과를 사용할 수 있습니다. Security Hub CSPM 콘솔의 제어 페이지에는 표준 전체의 모든 제어가 표시됩니다. 표준 전체에서 각 제어에는 동일한 제어 ID가 있습니다. 통합 제어 조사 결과를 켜면 제어가 활성화된 여러 표준에 적용되는 경우에도 보안 검사당 단일 조사 결과를 받게 됩니다. | 2023년 8월 28일 |
| 이스라엘(텔아비브) 리전에서 Security Hub CSPM 사용 가능 | 이제 이스라엘(텔아비브)에서 Security Hub CSPM을 사용할 수 있습니다. 이제 특정 보안 제어를 제외한 모든 Security Hub CSPM 기능을 이 리전에서 사용할 수 있습니다. 자세한 정보는 리전별 제어 가용성을 참조하세요. | 2023년 8월 8일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[Athena.1] Athena 워크그룹은 저장 시 암호화되어야 합니다”<br>• the section called “[DocumentDB.1] Amazon DocumentDB 클러스터는 저장 시 암호화되어야 합니다.”<br>• the section called “[DocumentDB.2] Amazon DocumentDB 클러스터에는 적절한 백업 보존 기간이 있어야 합니다.”<br>• the section called “[Neptune.1] Neptune DB 클러스터는 저장 시 암호화되어야 합니다.”<br>• the section called “[Neptune.2] Neptune DB 클러스터는 감사 로그를 CloudWatch Logs에 게시해야 합니다.”<br>• the section called “[Neptune.3] Neptune DB 클러스터 스냅샷은 퍼블릭이 아니어야 합니다.”<br>• the section called “[Neptune.4] Neptune DB 클러스터에는 삭제 방지 기능이 활성화되어 있어야 합니다.”<br>• the section called “[Neptune.5] Neptune DB 클러스터에 | 2023년 7월 28일 |

| | | |
|---|---|---|
| | 는 자동 백업이 활성화되어 있어야 합니다.”<br>• the section called “[Neptune .6] Neptune DB 클러스터 스냅샷은 저장 시 암호화되어야 합니다.”<br>• the section called “[Neptune .7] Neptune DB 클러스터에는 IAM 데이터베이스 인증이 활성화되어 있어야 합니다.”<br>• the section called “[Neptune .8] 태그를 스냅샷에 복사하도록 Neptune DB 클러스터를 구성해야 합니다.”<br>• the section called “[RDS.27] RDS DB 클러스터는 저장 시 암호화되어야 합니다.” | |
| 자동화 규칙 기준에 대한 새로운 연산자 | 이제 자동화 규칙 맵 및 문자열 기준에 CONTAINS 및 NOT_CONTAINS 비교 연산자를 사용할 수 있습니다. | 2023년 7월 25일 |
| 자동화 규칙 | 이제 Security Hub CSPM은 사용자가 지정한 기준을 바탕으로 조사 결과를 자동으로 업데이트하는 자동화 규칙을 제공합니다. | 2023년 6월 13일 |
| 새로운 타사 통합 | Snyk는 Security Hub CSPM에 조사 결과를 전송하는 새로운 서드 파티 통합입니다. | 2023년 6월 12일 |

| | | |
|---|---|---|
| 서비스 관리형 표준에 추가된 기존 보안 제어: AWS Control Tower | 서비스 관리형 표준에 다음과 같은 기존 Security Hub CSPM 제어가 추가되었습니다 AWS Control Tower.<br>• the section called “[Account.1]에 대한 보안 연락처 정보를 제공해야 합니다.AWS 계정”<br>• the section called “[APIGateway.8] API 게이트웨이 경로는 인증 유형을 지정해야 합니다.”<br>• the section called “[APIGateway.9] API Gateway V2 단계에 대한 액세스 로깅을 구성해야 합니다.”<br>• the section called “[CodeBuild.3] CodeBuild S3 로그는 암호화되어야 합니다.”<br>• the section called “[EC2.25] Amazon EC2 시작 템플릿은 네트워크 인터페이스에 퍼블릭 IP를 할당해서는 안 됩니다.”<br>• the section called “[ELB.1] Application Load Balancer는 모든 HTTP 요청을 HTTPS로 리디렉션하도록 구성되어야 합니다.”<br>• the section called “[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다”<br>• the section called “[SageMaker.2] SageMaker | 2023년 6월 12일 |

노트북 인스턴스는 사용자 지정 VPC에서 시작해야 합니다.”

- the section called “[SageMaker.3] 사용자는 SageMaker 노트북 인스턴스에 대한 루트 액세스 권한이 없어야 합니다.”
- the section called “[WAF.10] AWS WAF웹 ACLs에는 하나 이상의 규칙 또는 규칙 그룹이 있어야 합니다.”

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[ACM.2] ACM에서 관리하는 RSA 인증서는 최소 2,048비트의 키 길이를 사용해야 합니다.”<br>• the section called “[AppSync.2]AWS AppSync필드 수준 로깅이 활성화되어 있어야 합니다.”<br>• the section called “[CloudFront.13] CloudFront 배포는 오리진 액세스 제어를 사용해야 합니다.”<br>• the section called “[Elastic Beanstalk.3] Elastic Beanstalk는 로그를 CloudWatch로 스트리밍해야 합니다.”<br>• the section called “[S3.17] S3 범용 버킷은 저장 시 로 암호화해야 합니다. AWS KMS keys”<br>• the section called “[StepFunctions.1] Step Functions 상태 머신에는 로깅이 켜져 있어야 합니다.” | 2023년 6월 6일 |

| | | |
|---|---|---|
| 아시아 태평양(멜버른)에서 Security Hub CSPM 사용 가능 | 이제 아시아 태평양(멜버른)에서 Security Hub CSPM을 사용할 수 있습니다. 이제 특정 보안 제어를 제외한 모든 Security Hub CSPM 기능을 이 리전에서 사용할 수 있습니다. 자세한 정보는 리전별 제어 가용성을 참조하세요. | 2023년 5월 25일 |
| 조사 결과 기록 | Security Hub CSPM은 이제 지난 90일 동안의 조사 결과 기록을 추적할 수 있습니다. | 2023년 5월 4일 |
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다.<br>• the section called “[EKS.1] EKS 클러스터 엔드포인트는 공개적으로 액세스할 수 없어야 합니다.”<br>• the section called “[ELB.16] Application Load Balancer는 AWS WAF 웹 ACL과 연결되어야 합니다.”<br>• the section called “[Redshift.10] Redshift 클러스터는 저장 시 암호화되어야 합니다”<br>• the section called “[S3.15] S3 범용 버킷에는 Object Lock이 활성화되어 있어야 합니다.” | 2023년 3월 29일 |
| 통합 제어 조사 결과에 대한 지원 확대 | AWS v2.0.0의 자동 보안 응답은 이제 통합 제어 조사 결과를 지원합니다. | 2023년 3월 24일 |

| | | |
|---|---|---|
| 새로운에서 Security Hub CSPM 사용 가능 AWS 리전 | 이제 아시아 태평양(하이데라바드), 유럽(스페인) 및 유럽(취리히)에서 Security Hub CSPM을 사용할 수 있습니다. 이러한 리전에서 사용할 수 있는 제어에는 제한이 있습니다. | 2023년 3월 21일 |
| 관리형 정책 업데이트 | Security Hub CSPM은 `AWSSecurityHubServiceRolePolicy` 관리형 정책에서 기존 권한을 업데이트했습니다. | 2023년 3월 17일 |

| | | |
|---|---|---|
| NIST 800-53 표준에 대한 새로운 보안 제어 | Security Hub CSPM은 NIST 800-53 표준에 적용할 수 있는 다음 보안 제어를 추가했습니다.<br>• the section called “[Account.2] AWS Organizations조직의 일부여야 AWS 계정합니다.”<br>• the section called “[CloudWatch.15] CloudWatch 경보에는 지정된 구성되어 있어야 합니다.”<br>• the section called “[CloudWatch.16] CloudWatch 로그 그룹은 지정된 기간 동안 보존되어야 합니다.”<br>• the section called “[CloudWatch.17] CloudWatch 경보 조치를 활성화해야 합니다.”<br>• the section called “[DynamoDB.4] DynamoDB 테이블은 백업 계획에 있어야 합니다.”<br>• the section called “[EC2.28] EBS 볼륨에는 백업 계획이 적용되어야 합니다.”<br>• EC2.29 – EC2 인스턴스는 VPC에서 시작되어야 합니다(사용 중지됨).<br>• the section called “[RDS.26] RDS DB 인스턴스는 백업 계획으로 보호되어야 합니다.”<br>• the section called “[S3.14] S3 범용 버킷에는 버전 관리 | 2023년 3월 3일 |

| | | |
|---|---|---|
| | 가 활성화되어 있어야 합니다.”<br>• the section called “[WAF.11] AWS WAF웹 ACL 로깅을 활성화해야 합니다.” | |
| NIST(국립 표준 기술 연구소) 800-53 버전 5 | Security Hub CSPM은 이제 200개 이상의 적용 가능한 보안 제어를 사용해 NIST 800-53 버전 5 표준을 지원합니다. | 2023년 2월 28일 |
| 통합 제어 보기 및 제어 조사 결과 | 통합 제어 보기가 릴리스됨에 따라, Security Hub CSPM 콘솔의 제어 페이지에는 표준 전체의 모든 제어가 표시됩니다. 표준 전체에서 각 제어에는 동일한 제어 ID가 있습니다. 통합 제어 조사 결과를 켜면 제어가 활성화된 여러 표준에 적용되는 경우에도 보안 검사당 단일 조사 결과를 받게 됩니다. | 2023년 2월 23일 |

| | | |
|---|---|---|
| 새로운 보안 제어 | 다음 새로운 Security Hub CSPM 제어를 사용할 수 있습니다. 일부 제어에는 리전 제한이 있습니다.<br>• the section called “[ElastiCache.1] ElastiCache(Redis OSS) 클러스터에는 자동 백업이 활성화되어 있어야 합니다.”<br>• the section called “[ElastiCache.2] ElastiCache 클러스터에는 마이너 버전 자동 업그레이드가 활성화되어 있어야 합니다”<br>• the section called “[ElastiCache.3] ElastiCache 복제 그룹에는 자동 장애 조치가 활성화되어 있어야 합니다.”<br>• the section called “[ElastiCache.4] ElastiCache 복제 그룹은 저장 시 암호화해야 합니다.”<br>• the section called “[ElastiCache.5] ElastiCache 복제 그룹은 전송 중 암호화되어야 합니다.”<br>• the section called “[ElastiCache.6] 이전 버전의 ElastiCache(Redis OSS) 복제 그룹에는 Redis OSS AUTH가 활성화되어 있어야 합니다.”<br>• the section called “[ElastiCache.7] ElastiCache 클러스 | 2023년 2월 16일 |

| | | |
|---|---|---|
| | 터는 기본 서브넷 그룹을 사용해서는 안 됩니다.” | |
| 새로운 ASFF 필드 | Security Hub CSPM은 ProductFields.ArchivalReasons:0/Description 및 ProductFields.ArchivalReasons:0/ReasonCode를 AWS Security Finding Format(ASFF)에 추가했습니다. | 2023년 2월 8일 |
| 새로운 ASFF 필드 | Security Hub CSPM은 Security AWS Finding Format(ASFF)에 Compliance.AssociatedStandards 및 Compliance.SecurityControlId를 추가했습니다. | 2023년 1월 31일 |
| 이제 취약성 세부 정보 사용 가능 | 이제 Security Hub CSPM 콘솔에서 Amazon Inspector가 Security Hub CSPM로 전송하는 조사 결과에 대한 취약성 세부 정보를 볼 수 있습니다. | 2023년 1월 14일 |
| Security Hub CSPM을 중동(UAE)에서 사용 가능 | 이제 Security Hub CSPM을 중동(UAE)에서 사용할 수 있습니다. 일부 제어에는 리전 제한이 있습니다. | 2023년 1월 12일 |
| MetricStream과의 타사 통합 추가 | Security Hub CSPM은 이제 중국 및를 제외한 모든 리전 MetricStream에서 와의 타사 통합을 지원합니다 AWS GovCloud (US). | 2023년 1월 11일 |

| | | |
|---|---|---|
| 조직 계정 한도 확대 | Security Hub CSPM은 이제 리전당 각 Security Hub CSPM 관리자에 대해 최대 11,000개의 멤버 계정을 지원합니다. | 2022년 12월 27일 |
| ElasticBeanstalk.3 롤백 | Security Hub CSPM은 모든 리전에서 FSBP 표준으로부터 [ElasticBeanstalk.3] Elastic Beanstalk는 CloudWatch로 로그를 스트림해야 합니다 제어를 롤백했습니다. | 2022년 12월 21일 |
| Security Hub CSPM이 새로운 보안 제어 추가 | FSBP 표준을 활성화한 고객은 새로운 Security Hub CSPM 제어를 사용할 수 있습니다. 일부 제어에는 리전 제한이 있습니다. | 2022년 12월 15일 |
| 향후 기능에 대한 지침 | Security Hub CSPM은 통합 제어 보기와 통합 제어 조사 결과라는 두 가지 새로운 기능을 릴리스할 계획입니다. 곧 나올 이러한 기능은 제어 조사 결과 필드 및 값에 의존하는 기존 워크플로우에 영향을 미칠 수 있습니다. | 2022년 12월 9일 |
| 이제 Amazon Security Lake 사용 가능 | 이제 Security Lake는 Security Hub CSPM 조사 결과를 수신하여 Security Hub CSPM과 통합되었습니다. | 2022년 11월 29일 |

| | | |
|---|---|---|
| 서비스 관리형 표준 지원: AWS Control Tower | Security Hub CSPM은 서비스 관리형 표준:이라는 새로운 보안 표준을 지원합니다 AWS Control Tower. AWS Control Tower 는이 표준을 관리합니다. | 2022년 11월 28일 |
| 이제 중국 리전에서 CIS AWS 파운데이션 벤치마크 v1.4.0 사용 가능 | Security Hub CSPM은 이제 중국 리전에서 CIS AWS 파운데이션 벤치마크 v1.4.0을 지원합니다. | 2022년 11월 18일 |
| 이제 Jira Service Management Cloud 통합 사용 가능 | Jira Service Management Cloud는 이제 중국 리전을 제외하고 사용 가능한 모든 리전에서 Security Hub CSPM 조사 결과를 수신합니다. | 2022년 11월 17일 |
| AWS IoT Device Defender 이제 통합 사용 가능 | AWS IoT Device Defender 는 이제 사용 가능한 모든 리전의 Security Hub CSPM에 조사 결과를 전송합니다. | 2022년 11월 17일 |
| CIS AWS 파운데이션 벤치마크 v1.4.0 지원 | Security Hub CSPM은 이제 CIS AWS 파운데이션 벤치마크 v1.4.0을 지원하는 보안 제어를 제공합니다. 이 표준은 중국 리전을 제외한 모든 사용 가능한 리전에서 사용할 수 있습니다. | 2022년 11월 9일 |

| | | |
|---|---|---|
| 에서 Security Hub CSPM 발표 지원 AWS GovCloud (US) | 이제 AWS GovCloud(미국 동부) 및 AWS GovCloud(미국 서부)에서 Amazon Simple Notification Service(Amazon SNS)를 사용하여 Security Hub CSPM 공지를 구독하여 Security Hub CSPM에 대한 알림을 받을 수 있습니다. | 2022년 10월 3일 |
| AWS Security Hub CSPM에 새로운 보안 제어 추가 | FSBP 표준을 활성화한 고객은 새로운 Security Hub CSPM 제어 AutoScaling.9를 사용할 수 있습니다. 제어에는 리전 제한이 있을 수 있습니다. | 2022년 9월 1일 |
| Security Hub CSPM 공지 구독 | 이제 Amazon Simple Notification Service(Amazon SNS)를 통해 Security Hub CSPM 공지를 구독하여 Security Hub CSPM에 대한 알림을 받을 수 있습니다. | 2022년 8월 29일 |
| 교차 리전 집계 활성화를 위한 리전 확장 | 이제 교차 리전 집계 활성화를 조사 결과, 조사 결과 업데이트, AWS GovCloud (US)전체의 인사이트에 사용할 수 있습니다. | 2022년 8월 2일 |
| 새로운 타사 제품 통합 | Fortinet - FortiCNP는 Security Hub CSPM 조사 결과를 수신하는 서드 파티 통합이며, JFrog는 조사 결과를 Security Hub CSPM으로 전송하는 서드 파티 통합입니다. | 2022년 7월 26일 |

| | | |
|---|---|---|
| EC2.27은 사용 중지되었습니다 | Security Hub CSPM은 AWS 기본 보안 모범 사례(FSBP) 표준에서 이전의 EC2.27- EC2 인스턴스를 실행하는 데 키 페어를 사용해서는 안 됩니다 제어를 사용 중지했습니다. | 2022년 7월 20일 |
| Lambda.2는 더 이상 python3.6을 지원하지 않습니다 | Security Hub CSPM은 더 이상 Lambda.2의 파라미터로 python3.6을 지원하지 않습니다. Lambda 함수는 기본 보안 모범 사례(FSBP) 표준의 제어인 지원되는 런타임을 사용해야 합니다. AWS | 2022년 7월 19일 |
| AWS Security Hub CSPM이 새로운 보안 제어 추가 | FSBP 표준을 활성화한 고객은 새로운 Security Hub CSPM 제어를 사용할 수 있습니다. 일부 제어에는 리전 제한이 있습니다. | 2022년 6월 22일 |
| AWS Security Hub CSPM에서 새 리전 지원 | 이제 아시아 태평양(자카르타)에서 Security Hub CSPM을 사용할 수 있습니다. 일부 제어는 이 리전에서 사용할 수 없습니다. | 2022년 6월 7일 |
| AWS Security Hub CSPM과 간의 통합 개선 AWS Config | Security Hub CSPM 사용자는 Security Hub CSPM에서 AWS Config 규칙 평가 결과를 조사 결과로 볼 수 있습니다. | 2022년 6월 6일 |

| | | |
|---|---|---|
| 자동 활성화 표준을 옵트아웃하는 기능 추가 | 와를 통합한 사용자의 경우 AWS Organizations이 기능을 사용하면 Security Hub CSPM 관리자 계정에 로그인하고 자동 활성화 표준에서 새 멤버 계정을 옵트아웃할 수 있습니다. | 2022년 4월 25일 |
| 교차 리전 집계 활성화 확장 | 상태 및 보안 점수를 제어하기 위해 교차 리전 집계 활성화를 추가했습니다. | 2022년 4월 20일 |
| CompanyName 및 ProductName은 이제 최상위 속성임 | 사용자 지정 통합과 관련된 회사 및 제품 이름을 설정하기 위한 새로운 최상위 속성 추가 | 2022년 4월 1일 |
| AWS 기본 보안 모범 사례 표준에 새로운 제어 추가 | AWS 기본 보안 모범 사례 표준에 5가지 새로운 제어를 추가했습니다. | 2022년 3월 31일 |
| ASFF에 새로운 리소스 세부 정보 객체 추가 | ASFF에 `AwsRdsDbSecurityGroup` 리소스 유형이 추가되었습니다. | 2022년 3월 25일 |
| ASFF에 추가 리소스 세부 정보 추가 | `AwsAutoScalingScalingGroup` , `AwsElbLoadBalancer` , `AwsRedshiftCluster` 및 `AwsCodeBuildProject` 에 추가 세부 정보가 추가되었습니다. | 2022년 3월 25일 |
| AWS 기본 보안 모범 사례 표준에 새로운 제어 추가 | AWS 기본 보안 모범 사례 표준에 15개의 새로운 제어를 추가했습니다. | 2022년 3월 16일 |

| | | |
|---|---|---|
| AWS 기본 보안 모범 사례 표준 및 PCI DSS(지불 카드 산업 데이터 보안 표준)에 새로운 제어 기능 추가 | AWS Foundational Security Best Practices 표준에 Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing 및 CloudFront에 대한 새로운 제어를 추가했습니다. 또한 PCI DSS에 OpenSearch Service를 위한 두 가지 새로운 제어를 추가했습니다. | 2022년 2월 15일 |
| ASFF에 새로운 필드 추가 | 새로운 필드 추가: 샘플. | 2022년 1월 26일 |
| 와의 통합 추가 AWS Health | AWS Health 는 service-to-service 이벤트 메시징을 사용하여 조사 결과를 Security Hub CSPM으로 전송합니다. | 2022년 1월 19일 |
| 와의 통합 추가 AWS Trusted Advisor | Trusted Advisor 는 검사 결과를 Security Hub CSPM 조사 결과로 Security Hub CSPM에 전송합니다. Security Hub CSPM은 AWS 기본 보안 모범 사례 검사 결과를 로 전송합니다 Trusted Advisor. | 2022년 1월 18일 |

| | | |
|---|---|---|
| ASFF에서 리소스 세부 정보 객체 업데이트 | AwsAutoScalingAutoScalingGroup 에 MixedInstancesPolicy 및 AvailabilityZones 추가. AwsAutoScalingLaunchConfiguration 에 MetadataOptions 이(가) 추가되었습니다. AwsS3Bucket 에 BucketVersioningConfiguration 이(가) 추가되었습니다. | 2021년 12월 20일 |
| ASFF 설명서의 출력 업데이트 | 이전에는 ASFF 속성에 대한 설명이 단일 주제에 있었습니다. 이제 각 최상위 객체와 각 리소스 세부 정보 객체가 고유한 주제에 속합니다. ASFF 구문 주제에는 해당 항목에 대한 링크가 포함되어 있습니다. | 2021년 12월 20일 |
| 용 ASFF에 새 리소스 세부 정보 객체 추가 AWS Network Firewall | 에 AWS Network Firewall, AwsNetworkFirewallFirewall AwsNetworkFireFirewallPolicy 및 리소스 세부 정보 객체가 추가되었습니다AwsNetworkFirewallRuleGroup . | 2021년 12월 20일 |
| 새로운 버전의 Amazon Inspector에 대한 지원 추가 | Security Hub CSPM은 새로운 버전의 Amazon Inspector 및 Amazon Inspector Classic과 통합되었습니다. Amazon Inspector는 조사 결과를 Security Hub CSPM으로 전송합니다. | 2021년 11월 29일 |

| | | |
|---|---|---|
| EC2.19의 심각도 변경 | EC2.19의 심각도(보안 그룹은 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됨)가 높음에서 심각으로 변경되었습니다. | 2021년 11월 17일 |
| Sonrai Dig과의 새로운 통합 | Security Hub CSPM은 이제 Sonrai Dig와의 통합을 제공합니다. Sonrai Dig는 클라우드 환경을 모니터링하여 보안 위험을 식별합니다. Sonrai Dig은 조사 결과를 Security Hub CSPM으로 전송합니다. | 2021년 11월 12일 |
| CIS 2.1 및 CloudTrail.1 제어에 대한 점검 업데이트 | CIS 2.1 및 CloudTrail.1은 다중 리전 CloudTrail 트레일이 하나 이상 준비되었는지 확인하는 것 외에도 이제 다중 리전 CloudTrail 트레일 트레일 중 하나 이상에서 `ExcludeManagementEventSources` 파라미터가 비어 있는지 확인합니다. | 2021년 11월 9일 |
| VPC 엔드포인트에 대한 지원 추가 | Security Hub CSPM은 이제와 통합 AWS PrivateLink 되고 VPC 엔드포인트를 지원합니다. | 2021년 11월 3일 |
| AWS 기본 보안 모범 사례 표준에 제어 추가 | Elastic Load Balancing(ELB.2 및 ELB.8) 및 AWS Systems Manager (SSM.4)에 대한 새로운 제어가 추가되었습니다. | 2021년 11월 2일 |

| | | |
|---|---|---|
| EC2.19 제어 점검에 포트 추가 | 또한 EC2.19는 이제 보안 그룹이 3000(Go, Node.js, 루비 웹 개발 프레임워크), 5000(Python 웹 개발 프레임워크), 8088(레거시 HTTP 포트), 8888(대체 HTTP 포트) 포트에 대한 무제한 수신 액세스를 허용하지 않는지 점검합니다. | 2021년 10월 27일 |
| Logz.io Cloud SIEM과의 통합 추가 | Logz.io는 보안 팀이 보안 위협을 실시간으로 탐지, 분석 및 대응하는 데 도움을 주기 위해 로그 및 이벤트 데이터의 고급 상관 관계를 제공하는 Cloud SIEM 공급자입니다. Logz.io는 Security Hub CSPM에서 조사 결과를 수신합니다. | 2021년 10월 25일 |
| 조사 결과의 교차 리전 집계 활성화를 위한 지원 추가 | 교차 리전 집계 활성화를 사용하면 리전을 변경하지 않고도 모든 조사 결과를 볼 수 있습니다. 관리자 계정은 집계 리전 및 연결 리전을 선택합니다. 관리자 계정 및 해당 구성원 계정에 대한 조사 결과는 연결 리전에서 집계 리전으로 집계됩니다. | 2021년 10월 20일 |

| | | |
|---|---|---|
| ASFF에서 리소스 세부 정보 객체 업데이트 | AwsCloudFrontDistribution 에 뷰어 인증서 세부 정보가 추가되었습니다. AwsCodeBuildProject 에 추가 세부 정보가 추가되었습니다. AwsElbV2LoadBalancer 에 로드 밸런서 속성이 추가되었습니다. AwsS3Bucket 에 S3 버킷 소유자 계정 식별자가 추가되었습니다. | 2021년 10월 8일 |
| ASFF에 새로운 리소스 세부 정보 객체 추가 | ASFF에 AwsEc2VpcEndpointService , AwsEcrRepository , AwsEksCluster , AwsOpenSearchServiceDomain , AwsWafRateBasedRule , AwsWafRegionalRateBasedRule , AwsXrayEncryptionConfig 새로운 리소스 세부 정보 객체 추가 | 2021년 10월 8일 |
| Lambda.2 제어에서 더 이상 사용되지 않는 런타임 삭제 | AWS 기본 보안 모범 사례 표준에서는 [Lambda.2] Lambda 함수에서 지원되는 dotnetcore2.1 런타임을 사용해야 하는 런타임을 제거했습니다. | 2021년 10월 6일 |
| Check Point 통합에 새로운 이름 | Check Point Dome9 Arc와의 통합은 이제 Check Point CloudGuard Posture Management입니다. 통합 ARN은 변경되지 않았습니다. | 2021년 10월 1일 |

| | | |
|---|---|---|
| Alcide와의 통합 삭제됨 | Alcide KAudit과의 통합이 중단되었습니다. | 2021년 9월 30일 |
| EC2.19의 심각도 변경 | [EC2.19]의 보안 그룹의 경우, 위험이 높은 포트에 대한 무제한 액세스를 허용해서는 안 됩니다의 심각도는 중간에서 높음으로 변경되었습니다. | 2021년 9월 30일 |
| AWS Organizations 이제 중국 리전에서 와의 통합이 지원됩니다. | 이제 중국(베이징) 및 중국(닝샤)에서 Security Hub CSPM과 Organizations의 통합을 지원합니다. | 2021년 9월 20일 |
| S3.1 및 PCI.S3.6 제어에 대한 새 AWS Config 규칙 | S3.1 및 PCI.S3.6 모두 Amazon S3 Block Public Access 설정이 활성화되어 있는지 확인합니다. 이러한 제어에 대한 AWS Config 규칙이 에서 `s3-account-level-public-access-blocks` 로 변경됩니다`s3-account-level-public-access-blocks-periodic` . | 2021년 9월 14일 |
| Lambda.2 제어에서 더 이상 사용되지 않는 런타임 삭제 | AWS 기본 보안 모범 사례 표준에서 [Lambda.2] Lambda 함수가 지원되는 `ruby2.5` 런타임을 사용해야 하는 `nodejs10.x` 및 런타임을 제거했습니다. | 2021년 9월 13일 |
| CIS 2.2 제어의 심각도 변경 | CIS AWS 파운데이션 벤치마크 표준에서 2.2의 심각도입니다. - CloudTrail 로그 파일 검증이 활성화되었는지 여부를 확인합니다의 심각도가 낮음에서 중간으로 변경되었습니다. | 2021년 9월 13일 |

| | | |
|---|---|---|
| AWS 기본 보안 모범 사례 표준의 ECS.1, Lambda.2 및 SSM.1 업데이트 | AWS 기본 보안 모범 사례 표준에서 ECS.1에는 이제 로 설정된 `SkipInactiveTaskDefinitions` 파라미터가 있습니다`true`. 이렇게 하면 제어가 활성 작업 정의만 점검할 수 있습니다. Lambda.2의 경우, 런타임 목록에 Python 3.9를 추가. SSM.1은 이제 중지된 인스턴스와 실행 중인 인스턴스를 모두 점검합니다. | 2021년 9월 7일 |
| 이제 PCI.Lambda.2 제어에서 Lambda @Edge 리소스가 제외됩니다. | 이제 PCI DSS(지불 카드 산업 데이터 보안 표준) 표준에서는 이제 PCI.Lambda.2 제어에서 Lambda @Edge 리소스가 제외됩니다. | 2021년 9월 7일 |
| HackerOne Vulnerability Intelligence와(과)의 통합 추가 | Security Hub CSPM은 이제 HackerOne Vulnerability Intelligence와의 통합을 제공합니다. 이 통합은 조사 결과를 Security Hub CSPM으로 전송합니다. | 2021년 9월 7일 |
| ASFF에서 리소스 세부 정보 객체 업데이트 | `AwsKmsKey` 에 대해 `KeyRotationStatus` 추가. `AwsS3Bucket` 에 대해 `AccessControlList` , `BucketLoggingConfiguration` , `BucketNotificationConfiguration` , `BucketWebsiteConfiguration` 추가. | 2021년 9월 2일 |

| | | |
|---|---|---|
| ASFF에 새로운 리소스 세부 정보 객체 추가 | ASFF에 AwsAutoScalingLaunchConfiguration , AwsEc2VpnConnection , AwsEcrContainerImage 새로운 리소스 세부 정보 객체가 추가되었습니다 | 2021년 9월 2일 |
| ASFF에서 Vulnerabilities 객체에 세부 정보 추가 | Cvss에서 Adjustments 및 Source 추가 VulnerablePackages 에서 파일 경로와 패키지 관리자 추가 | 2021년 9월 2일 |
| 이제 중국 리전에서 Systems Manager 탐색기와 OpsCenter 통합이 지원 | 이제 중국(베이징) 및 중국(닝샤)에서 Security Hub CSPM과 SSM Explorer and OpsCenter의 통합을 지원합니다. | 2021년 8월 31일 |
| Lambda.4 제어 사용 중지 | Security Hub CSPM은 [Lambda.4] Lambda 함수에는 Dead Letter Queue(DLQ)가 구성되어 있어야 합니다 제어를 사용 중지합니다. 제어가 사용 중지되면 콘솔에 더 이상 표시되지 않으며 Security Hub CSPM은 이에 대한 확인을 수행하지 않습니다. | 2021년 8월 31일 |
| PCI.EC2.3 제어 사용 중지 | Security Hub CSPM은 [PCI.EC2.3] 사용하지 않는 EC2 보안 그룹은 삭제해야 합니다 제어를 사용 중지합니다. 제어가 사용 중지되면 콘솔에 더 이상 표시되지 않으며 Security Hub CSPM은 이에 대한 확인을 수행하지 않습니다. | 2021년 8월 27일 |

| | | |
|---|---|---|
| Security Hub CSPM이 조사 결과를 사용자 지정 작업에 전송하는 방식 변경 | 조사 결과를 사용자 지정 작업에 전송할 때 Security Hub CSPM은 이제 각 조사 결과를 별도의 Security Hub Findings - Custom Action 이벤트에서 전송합니다. | 2021년 8월 20일 |
| 사용자 지정 Lambda 런타임에 대한 새로운 규정 준수 상태 사유 코드 추가 | 새로운 `LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE` 규정 준수 상태 사유 코드 추가 이 사유 코드는 Security Hub CSPM이 사용자 지정 Lambda 런타임에 대해 점검을 수행할 수 없음을 나타냅니다. | 2021년 8월 20일 |
| AWS Firewall Manager 이제 중국 리전에서 통합 지원 | 이제 중국(베이징) 및 중국(닝샤)에서 Security Hub CSPM과 Firewall Manager의 통합을 지원합니다. | 2021년 8월 19일 |
| Caveonix Cloud 및 Forcepoint Cloud Security Gateway와(과)의 새로운 통합 | Security Hub CSPM은 이제 Caveonix Cloud 및 Forcepoint Cloud Security Gateway와의 통합을 제공합니다. 두 통합 모두 Security Hub CSPM으로 조사 결과를 전송합니다. | 2021년 8월 10일 |

| | | |
|---|---|---|
| ASFF에 새로운 CompanyName , ProductName 및 Region 속성이 추가 | ASFF의 최상위 레벨에 CompanyName , ProductName , 및 Region 필드 추가 이러한 필드는 자동으로 채워지며 사용자 지정 제품 통합을 제외하고 BatchImportFindings 또는 BatchUpdateFindings 를 사용하여 업데이트할 수 없습니다. 콘솔에서 조사 결과 필터는 이러한 새로운 필드를 사용합니다. API에서 CompanyName 및 ProductName 필터는 ProductFields 아래에 있는 속성을 사용합니다. | 2021년 7월 23일 |
| ASFF에서 리소스 세부 정보 객체 추가 및 업데이트 | 새로운 AwsRdsEventSubscription 리소스 유형 및 새로운 리소스 세부 정보가 추가되었습니다. AwsEcsService 리소스 유형에 대한 리소스 세부 정보가 추가되었습니다. AwsElasticsearchDomain 리소스 세부 정보 객체에 속성이 추가되었습니다. | 2021년 7월 23일 |

| | | |
|---|---|---|
| AWS 기본 보안 모범 사례 표준에 제어 추가 | Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon OpenSearch Service (ES.5~ES.8), Amazon RDS(RDS.16~RDS.23), Amazon Redshift (Redshift.4), Amazon SQS (SQS.1)에 대해 새로운 제어를 추가했습니다. | 2021년 7월 20일 |
| 서비스 연결 역할 관리형 정책 내에서 권한 이동 | 관리형 정책 `AWSSecurityHubServiceRolePolicy` 내에서 `config:PutEvaluations` 권한을 이동함으로써, 모든 리소스에 적용됩니다. | 2021년 7월 14일 |
| AWS 기본 보안 모범 사례 표준에 제어 추가 | Amazon API Gateway (APIGateway.4), Amazon CloudFront (CloudFront.5 및 CloudFront.6), Amazon EC2 (EC2.17 및 EC2.18), Amazon ECS (ECS.1), Amazon OpenSearch Service (ES.4), AWS Identity and Access Management (IAM.21), Amazon RDS (RDS.15), Amazon S3 (S3.8)에 대한 새로운 제어를 추가했습니다. | 2021년 7월 8일 |

| | | |
|---|---|---|
| 제어 조사 결과에 대한 새로운 규정 준수 상태 사유 코드 추가 | `INTERNAL_SERVICE_ERROR` 는 알 수 없는 오류가 발생했음을 나타냅니다. `SNS_TOPIC_CROSS_ACCOUNT` 는 SNS 주제를 다른 계정에서 소유하고 있음을 나타냅니다. `SNS_TOPIC_INVALID` 는 연결된 SNS 주제가 유효하지 않음을 나타냅니다. | 2021년 7월 6일 |
| 채팅 애플리케이션의 Amazon Q Developer와의 통합 추가 | 채팅 애플리케이션의 Amazon Q Developer와의 통합이 추가되었습니다. Security Hub CSPM은 조사 결과를 채팅 애플리케이션의 Amazon Q Developer로 전송합니다. | 2021년 6월 30일 |
| 서비스 연결 역할 관리형 정책에 새로운 권한 추가 | 서비스 연결 역할이 평가 결과를 AWS Config에 제공할 수 있도록 허용하는 새로운 권한을 관리형 `AWSSecurityHubServiceRolePolicy` 정책에 추가했습니다. | 2021년 6월 29일 |
| ASFF에서 새로운 리소스 세부 정보 객체 추가 및 업데이트 | ECS 클러스터 및 ECS 작업 정의에 대한 새로운 리소스 세부 정보 객체가 추가되었습니다. 연결된 네트워크 인터페이스를 나열하도록 EC2 인스턴스 객체가 업데이트되었습니다. API Gateway V2 단계에 대한 클라이언트 인증서 ID가 추가되었습니다. S3 버킷의 수명 주기 구성이 추가되었습니다. | 2021년 6월 24일 |

| | | |
|---|---|---|
| 집계된 제어 상태 및 표준 보안 점수 계산 업데이트 | Security Hub CSPM은 이제 24시간마다 전체 제어 상태와 표준 보안 점수를 계산합니다. 관리자 계정의 경우, 이제 각 계정에 대한 각 제어의 활성화 또는 비활성화 여부가 점수에 반영됩니다. | 2021년 6월 23일 |
| Security Hub CSPM의 일시 중지된 계정 처리에 대한 정보 업데이트 | Security Hub CSPM이 AWS에서 일시 중지된 계정을 처리하는 방법에 대한 정보가 추가되었습니다. | 2021년 6월 23일 |
| 개별 관리자 계정의 활성화된 컨트롤과 비활성화된 제어를 표시하는 탭 추가 | 관리자 계정의 경우, 표준 세부 정보 페이지의 기본 탭에는 계정 전체에 대한 집계 정보가 포함됩니다. 새로운로 추가된 이 계정에 대해 활성화됨 및 이 계정에 대해 비활성화됨 탭에는 개별 관리자 계정에 대해 활성화되거나 비활성화된 계정이 나열됩니다. | 2021년 6월 23일 |
| `Lambda.2`에 대한 파라미터에 `java8.al2` 추가 | AWS 기본 보안 모범 사례 표준에서 `Lambda.2` 제어`java8.al2` 에 대해 지원되는 런타임에가 추가되었습니다. | 2021년 6월 8일 |

| | | |
|---|---|---|
| MicroFocus ArcSight 및 NETSCOUT Cyber Investigator와의 새로운 통합 | MicroFocus ArcSight 및 NETSCOUT Cyber Investigator와의 새 통합이 추가되었습니다. MicroFocus ArcSight는 Security Hub CSPM에서 조사 결과를 수신합니다. NETSCOUT Cyber Investigator는 Security Hub CSPM로 조사 결과를 전송합니다. | 2021년 6월 7일 |
| AWSSecurityHubServiceRolePolicy 에 대한 세부 정보 추가 | Security Hub CSPM 서비스 연결 역할에서 사용하는 기존 관리형 정책 `AWSSecurityHubServiceRolePolicy` 에 대한 세부 정보를 추가하도록 관리형 정책 섹션을 업데이트했습니다. | 2021년 6월 4일 |
| Jira Service Management와의 새로운 통합 | AWS Service Management Connector for Jira는 조사 결과를 Jira로 전송하고 이를 사용하여 Jira 문제를 생성합니다. Jira 문제가 업데이트되면 Security Hub CSPM의 해당 조사 결과도 업데이트됩니다. | 2021년 5월 26일 |
| 아시아 태평양(오사카) 리전에서 지원되는 제어 목록 업데이트 | 아시아 태평양(오사카)에서 지원되지 않는 제어를 나타내도록 CIS AWS 파운데이션 표준 및 PCI DSS(지불 카드 산업 데이터 보안 표준)를 업데이트했습니다. | 2021년 5월 21일 |
| 클라우드용 Sysdig Secure와의 새로운 통합 | 클라우드용 Sysdig Secure와의 통합이 추가되었습니다. 이 통합은 조사 결과를 Security Hub CSPM으로 전송합니다. | 2021년 5월 14일 |

| | | |
|---|---|---|
| AWS 기본 보안 모범 사례 표준에 제어 추가 | Amazon API Gateway(APIGateway.2 및 APIGateway.3), AWS CloudTrail (CloudTrail.4 및 CloudTrail.5), Amazon EC2(EC2.15 및 EC2.16), AWS Elastic Beanstalk (ElasticBeanstalk.1 및 ElasticBeanstalk.2), AWS Lambda (Lambda.4), Amazon RDS(RDS.12 – RDS.14), Amazon Redshift(Redshift.7), AWS Secrets Manager (SecretsManager.3 및 SecretsManager.4), 및 AWS WAF (WAF.1)에 대한 새로운 제어가 추가되었습니다. | 2021년 5월 10일 |
| GuardDuty 및 Amazon RDS 제어 추가 | `GuardDuty.1` 및 `PCI.GuardDuty.1` 의 심각도를 중간에서 높음으로 변경했습니다. `RDS.8`에 `databaseEngines` 파라미터를 추가했습니다. | 2021년 5월 4일 |
| ASFF에 새로운 리소스 세부 정보 추가 | 에서 Amazon EC2 네트워크 ACL, Amazon EC2 서브넷 및 AWS Elastic Beanstalk 환경에 대한 새 리소스 세부 정보 객체를 `Resources.Details` 추가했습니다. ACLs | 2021년 5월 3일 |
| Amazon EventBridge 규칙에 대한 필터 값을 제공하는 콘솔 필드 추가 | Security Hub CSPM EventBridge 규칙에 대한 새로운 사전 정의된 필터 패턴은 필터 값을 지정하는 데 사용할 수 있는 콘솔 필드를 제공합니다. | 2021년 4월 30일 |

| | | |
|---|---|---|
| AWS Systems Manager Explorer 및 OpsCenter와의 통합 추가 | 이제 Security Hub CSPM은 Systems Manager Explorer 및 OpsCenter 와의 통합을 지원합니다. 통합은 Security Hub CSPM으로부터 조사 결과를 수신하고 Security Hub CSPM에서 이러한 조사 결과를 업데이트합니다. | 2021년 4월 26일 |
| 제품 통합의 새로운 유형 | 새로운 통합 유형인 `UPDATE_FINDINGS_IN_SECURITY_HUB` 은 제품 통합이 Security Hub CSPM으로부터 수신한 조사 결과를 업데이트한다는 것을 나타냅니다. | 2021년 4월 22일 |
| “마스터 계정”이 “관리자 계정”으로 변경 | ‘마스터 계정’이라는 용어가 ‘관리자 계정’으로 변경되었습니다. Security Hub CSPM 콘솔 및 API에서도 이 용어가 변경되었습니다. | 2021년 4월 22일 |
| HTTP를 Websocket으로 대체하도록 APIGateway.1을 업데이트 | API Gateway.1의 제목, 설명 및 문제 해결을 업데이트했습니다. 이제 제어에서 HTTP API 실행 로깅 대신 Websocket API 실행 로깅에 대해 확인합니다. | 2021년 4월 9일 |
| 베이징 및 닝샤에서 이제 Amazon GuardDuty 통합이 지원 | 이제 중국(베이징) 및 중국(닝샤) 리전에서 Security Hub CSPM과 GuardDuty의 통합이 지원됩니다. | 2021년 4월 5일 |
| Lambda.2 제어를 위해 지원되는 런타임에 `nodejs14.x` 추가 | Foundational Security Best Practices 표준의 Lambda.2 제어가 이제 `nodejs14.x` 런타임을 지원합니다. | 2021년 3월 30일 |

| | | |
|---|---|---|
| 아시아 태평양(오사카)에 Security Hub CSPM 출시 | 이제 아시아 태평양(오사카) 리전에서 Security Hub CSPM을 사용할 수 있습니다. | 2021년 3월 29일 |
| 조사 결과 세부 정보에 조사 결과 공급자 필드 추가 | 조사 결과 세부 정보 패널에서 새로운 공급자 필드 찾기 섹션에는 신뢰도, 중요도, 관련 조사 결과, 심각도 및 유형에 대한 조사 결과 제공자 값이 포함되어 있습니다. | 2021년 3월 24일 |
| Amazon Macie로부터 민감한 조사 결과를 받는 옵션 추가 | 이제 Macie와의 통합을 구성하여 민감한 조사 결과를 Security Hub CSPM으로 전송할 수 있습니다. | 2021년 3월 23일 |
| 계정 관리를 AWS Organizations 위해 로 전환 | 멤버 계정이 있는 기존 관리자 계정을 보유한 고객에 대해서는 초대를 통해 계정 관리에서 Organizations를 사용한 계정 관리로 변경하는 방법에 대한 새로운 정보가 추가되었습니다. | 2021년 3월 22일 |
| Amazon S3 퍼블릭 액세스 블록 구성에 대한 정보에 대해 ASFF에서 새로운 객체 | `Resources` 에서 새로운 `AwsS3AccountPublicAccessBlock` 리소스 유형 및 세부 정보 객체는 계정에 대한 Amazon S3 퍼블릭 액세스 블록 구성에 대한 정보를 제공합니다. `AwsS3Bucket` 리소스 세부 정보 객체에서 `PublicAccessBlockConfiguration` 객체는 S3 버킷에 퍼블릭 액세스 블록 구성을 제공합니다. | 2021년 3월 18일 |

| | | |
|---|---|---|
| 특정 필드를 업데이트할 조사 결과 공급자를 찾을 수 있도록 하는 ASFF의 새로운 객체 | ASFF의 새로운 FindingProviderFields 객체는 Confidence , Criticality , RelatedFindings , Severity, Types에 대한 값을 제공하는 BatchImportFindings 에 사용됩니다. 원래 필드는 BatchUpdateFindings 를 사용해서만 업데이트해야 합니다. | 2021년 3월 18일 |
| ASFF에서 리소스에 대한 새로운 DataClassification 객체 | ASFF에서 새로운 Resources.DataClassification 객체는 리소스에서 탐지된 민감한 데이터에 대한 정보를 제공하는 데 사용됩니다. | 2021년 3월 18일 |
| 사용 가능한 규정 준수 상태 코드에 CONFIG_RETURNS_NOT_APPLICABLE 값 추가 | NOT_AVAILABLE 규정 준수 상태의 경우, 사유 코드 RESOURCE_NO_LONGER_EXISTS 을(를) 삭제하고 사유 코드 CONFIG_RETURNS_NOT_APPLICABLE 을(를) 추가했습니다. | 2021년 3월 16일 |
| 와의 통합을 위한 새로운 관리형 정책 AWS Organizations | 새로운 관리형 정책 AWSSecurityHubOrganizationsAccess 은 조직 관리 계정과 위임된 Security Hub CSPM 관리자 계정에 필요한 Organizations 권한을 제공합니다. | 2021년 3월 15일 |

| | | |
|---|---|---|
| 관리형 정책 및 서비스 연결 역할 정보가 보안 장으로 이동 | 관리형 정책에 대한 정보가 개정 및 확장되었습니다. 관리형 정책 정보와 서비스 연결 역할에 대한 정보가 모두 보안 장으로 이동했습니다. | 2021년 3월 15일 |
| CIS 1.1 및 CIS 3.1 - CIS 3.14 제어에 대한 심각도 수정 | CIS 1.1 및 CIS 3.1 - CIS 3.14 제어의 심각도가 낮음으로 변경되었습니다. | 2021년 3월 3일 |
| RDS.11 제어 삭제 | Foundational Security Best Practices 표준에서 RDS.11 제어를 삭제했습니다. | 2021년 3월 3일 |
| Turbot에 대한 통합 업데이트 | Turbot 통합이 조사 결과를 보내고 받을 수 있도록 업데이트되었습니다. | 2021년 2월 26일 |
| Foundational Security Best Practices 표준에 제어 추가 | Amazon API Gateway(APIGateway.1), Amazon EC2(EC2.9 및 EC2.10), Amazon Elastic File System(EFS.2), Amazon OpenSearch Service(ES.2 및 ES.3), Elastic Load Balancing(ELB.6), AWS Key Management Service (AWS KMS)(KMS.3)에 대한 새로운 제어를 추가했습니다. | 2021년 2월 11일 |
| `DescribeProducts` API에 선택적 `ProductArn` 필터 추가 | 이제 `DescribeProducts` API 작업에 선택적 `ProductArn` 파라미터가 포함됩니다. `ProductArn` 파라미터는 세부 정보를 반환할 특정 제품 통합을 식별하는 데 사용됩니다. | 2021년 2월 3일 |

| | | |
|---|---|---|
| Cloud Storage Security의 Amazon S3용 안티바이러스와의 새로운 통합 | Amazon S3용 안티바이러스와의 통합은 바이러스 스캔 조사 결과를 Security Hub CSPM에 조사 결과로 전송합니다. | 2021년 1월 27일 |
| 관리자 계정의 보안 점수 계산 프로세스 업데이트 | 관리자 계정에서 Security Hub CSPM은 별도의 프로세스를 사용하여 보안 점수를 계산합니다. 새로운 프로세스에서는 멤버 계정에는 활성화되지만 관리자 계정에서는 비활성화된 제어가 점수에 포함되도록 합니다. | 2021년 1월 21일 |
| ASFF의 새로운 필드 및 객체 | 리소스에 대해 발생한 작업을 추적하는 새로운 `Action` 객체를 추가했습니다. DNS 이름과 IP 주소를 추적하는 필드를 `AwsEc2NetworkInterface` 객체에 추가했습니다. 리소스 세부 정보에 새로운 `AwsSsmPatchCompliance` 속성을 추가했습니다. | 2021년 1월 21일 |
| Foundational Security Best Practices 표준에 제어 추가 | Amazon CloudFront(CloudFront.1~CloudFront.4), Amazon DynamoDB(DynamoDB.1~DynamoDB.3), Elastic Load Balancing(ELB.3~ELB.5), Amazon RDS(RDS.9~RDS.11), Amazon Redshift(Redshift.1~Redshift.3 and Redshift.6), Amazon SNS(SNS.1)에 대한 새로운 제어를 추가했습니다. | 2021년 1월 15일 |

| | | |
|---|---|---|
| 워크플로우 상태는 기록 상태 또는 규정 준수 상태에 따라 재설정됩니다 | Security Hub CSPM은 보관된 조사 결과가 활성화되거나 조사 결과의 규정 준수 상태가 PASSED에서 FAILED, WARNING 또는 NOT_AVAILABLE 중 하나로 변경되는 경우, 워크플로 상태를 NOTIFIED 또는 RESOLVED에서 NEW로 자동으로 재설정합니다. 이러한 변경은 추가 조사가 필요함을 나타냅니다. | 2021년 1월 7일 |
| 제어 기반 조사 결과에 ProductFields 정보 추가 | 컨트롤에서 생성된 결과의 경우 AWS Security Finding Format(ASFF)에 ProductFields 객체 콘텐츠에 대한 정보가 추가되었습니다. | 2020년 12월 29일 |
| 관리형 인사이트 업데이트 | 인사이트 5의 제목 변경. 의심스러운 활동이 있는 IAM 사용자를 점검하는 새로운 인사이트 32가 추가되었습니다. | 2020년 12월 22일 |
| IAM.7 및 Lambda.1 제어에 대한 업데이트 | AWS 기본 보안 모범 사례 표준에서 IAM.7에 대한 파라미터를 업데이트했습니다. Lambda.1의 제목과 설명을 업데이트했습니다. | 2020년 12월 22일 |
| ServiceNow ITSM과의 확장된 통합 | ServiceNow ITSM 통합을 통해 사용자는 Security Hub CSPM 조사 결과를 수신하면 자동으로 인시던트 또는 문제를 생성할 수 있습니다. 이러한 인시던트 또는 문제가 업데이트되면 Security Hub CSPM의 조사 결과도 업데이트됩니다. | 2020년 12월 11일 |

| | | |
|---|---|---|
| AWS Audit Manager와의 새로운 통합 | Security Hub CSPM은 이제 AWS Audit Manager와의 통합을 제공합니다. 통합을 통해 Audit Manager는 Security Hub CSPM으로부터 제어 기반 조사 결과를 수신할 수 있습니다. | 2020년 12월 8일 |
| Aqua Security Kube-bench와의 새로운 통합 | Security Hub CSPM은 Aqua Security Kube-bench와의 통합을 추가했습니다. 이 통합은 조사 결과를 Security Hub CSPM으로 전송합니다. | 2020년 11월 24일 |
| 이제 중국 리전에서 Cloud Custodian을 사용할 수 있습니다 | 이제 중국(베이징) 및 중국(닝샤) 리전에서 Cloud Custodian과의 통합을 사용할 수 있습니다. | 2020년 11월 24일 |
| `BatchImportFindings` 는 이제 추가 필드를 업데이트하는 데 사용할 수 있습니다 | 이전에는, `Confidence` , `Criticality` , `RelatedFindings` , `Severity`, `Types` 필드를 업데이트하는 데 `BatchImportFindings` 을 사용할 수 없었습니다. 이제 이러한 필드를 `BatchUpdateFindings` 에 의해 업데이트하지 않은 경우, `BatchImportFindings` (으)로 업데이트할 수 있습니다. `BatchUpdateFindings` 에 의해 업데이트된 후에는 `BatchImportFindings` 로 업데이트할 수 없습니다. | 2020년 11월 24일 |

| | | |
|---|---|---|
| Security Hub CSPM이 이제와 통합됨 AWS Organizations | 이제 고객은 Organizations 계정 구성을 사용하여 구성원 계정을 관리할 수 있습니다. 조직 관리 계정은 Security Hub CSPM 관리자 계정으로 지정하고, 이 계정이 Security Hub CSPM에서 활성화할 조직 계정을 결정합니다. 조직의 일부가 아닌 계정에도 수동 초대 프로세스를 계속 사용할 수 있습니다. | 2020년 11월 23일 |
| 대용량 제어에 대한 별도의 조사 결과 목록 형식 삭제. | 조사 결과가 매우 많으면 제어의 조사 결과 목록에서 더 이상 조사 결과 페이지 형식을 사용하지 않습니다. | 2020년 11월 19일 |
| 신규 및 업데이트된 타사 통합 | Security Hub CSPM은 이제 cloudtamer.io, 3CORESec, Prowler, StackRox Kubernetes Security와의 통합을 지원합니다. IBM QRadar는 더 이상 조사 결과를 전송하지 않습니다. 이는 조사 결과를 수신만 합니다. | 2020년 10월 30일 |
| 제어 세부 정보 페이지에서 조사 결과를 다운로드하는 옵션이 추가되었습니다. | 제어 세부 정보 페이지에서 새로운 다운로드 옵션을 사용하여 조사 결과 목록을 .csv 파일로 다운로드할 수 있습니다. 다운로드한 목록은 목록에 있는 모든 필터를 따릅니다. 특정 조사 결과를 선택한 경우, 다운로드한 목록에는 해당 조사 결과만 포함됩니다. | 2020년 10월 26일 |

| | | |
|---|---|---|
| 표준 세부 정보 페이지에서 제어 목록을 다운로드하는 옵션이 추가되었습니다. | 표준 세부 정보 페이지에서 새로운 다운로드 옵션을 사용하여 제어 목록을 .csv 파일로 다운로드할 수 있습니다. 다운로드한 목록은 목록에 있는 모든 필터를 따릅니다. 특정 제어를 선택한 경우, 다운로드한 목록에는 해당 제어만 포함됩니다. | 2020년 10월 26일 |
| 신규 및 업데이트된 파트너 통합 | 이제 Security Hub CSPM이 ThreatModeler와 통합됩니다. 새로운 제품 이름을 반영하도록 다음 파트너 통합을 업데이트했습니다. Twistlock Enterprise Edition은 이제 Palo Alto Networks - Prisma Cloud Compute입니다. 또한 Palo Alto Networks에서 Demisto는 이제 Cortex XSOAR이고 Redlock은 이제 Prisma Cloud Enterprise입니다. | 2020년 10월 23일 |
| Security Hub CSPM이 중국(베이징) 및 중국(닝샤)에서 출시 | 이제 중국(베이징) 및 중국(닝샤) 리전에서 Security Hub CSPM을 사용할 수 있습니다. | 2020년 10월 21일 |
| ASFF 속성 및 타사 통합에 대한 형식 수정 | ASFF 속성 및 파트너 통합 목록은 이제 표 대신 목록 기반 형식을 사용합니다. ASFF 구문, 속성 및 유형 분류는 이제 별도의 주제에 있습니다. | 2020년 10월 15일 |
| 새롭게 디자인된 표준 세부 정보 페이지 | 활성화된 표준에 대한 표준 세부 정보 페이지에 이제 제어 탭 목록이 표시됩니다. 탭은 제어 상태를 기반으로 제어 목록을 필터링합니다. | 2020년 10월 7일 |

| | | |
|---|---|---|
| CloudWatch Events를 EventBridge로 대체 | Amazon CloudWatch Events에 대한 참조를 Amazon EventBridge로 대체했습니다. | 2020년 10월 1일 |
| Blue Hexagon for AWS, Alcide kAudit 및 Palo Alto Networks VM-Series와의 새로운 통합. | Security Hub CSPM이 이제 블루 육각형 for AWS, Alcide kAudit 및 Palo Alto Networks VM 시리즈와 통합되었습니다. AWS 및 kAudit용 블루 육각은 Security Hub CSPM으로 조사 결과를 보냅니다. VM-Series는 Security Hub CSPM으로부터 조사 결과를 수신합니다. | 2020년 9월 30일 |
| ASFF에서 새로운 리소스 세부 정보 객체 추가 및 업데이트 | `AwsApiGatewayRestApi` , `AwsApiGatewayStage` , `AwsApiGatewayV2Api` , `AwsApiGatewayV2Stage` , `AwsCertificateManagerCertificate` , `AwsElbLoadBalancer` , `AwsIamGroup` , `AwsRedshiftCluster` 에 대한 새로운 `Resources.Details` 객체를 추가하였습니다. `AwsCloudFrontDistribution` , `AwsIamRole` 및 `AwsIamAccessKey` 객체에 세부 정보가 추가되었습니다. | 2020년 9월 30일 |
| 리소스가 행위자인지 대상인지 추적하기 위한 ASFF의 리소스에 대한 새로운 `ResourceRole` 속성. | 리소스에 대한 `ResourceRole` 속성은 리소스가 조사 결과 활동의 대상인지 또는 조사 결과 활동의 가해자인지를 나타냅니다. 유효 값은 `ACTOR` 및 `TARGET`입니다. | 2020년 9월 30일 |

| | | |
|---|---|---|
| 사용 가능한 AWS 서비스 통합에 AWS Systems Manager 패치 관리자 추가 | AWS Systems Manager 이제 패치 관리자가 Security Hub CSPM과 통합되었습니다. Patch Manager는 고객의 플릿에 있는 인스턴스가 패치 규정 준수 표준을 위반하는 경우, Security Hub CSPM에 조사 결과를 전송합니다. | 2020년 9월 22일 |
| AWS 기본 보안 모범 사례 표준에 새로운 제어 추가 | Amazon EC2(EC2.7 및 EC2.8), Amazon EMR(EMR.1), IAM(IAM.8), Amazon RDS(RDS.4~RDS.8), Amazon S3(S3.6), AWS Secrets Manager (SecretsManager.1 및 SecretsManager.2)에 대한 새로운 제어가 추가되었습니다. | 2020년 9월 15일 |
| BatchUpdateFindings 필드에 대한 액세스를 제어하는 IAM 정책에 대한 새로운 컨텍스트 키 | 이제 BatchUpdateFindings 사용 시 필드 및 필드 값에 대한 액세스를 제한하도록 IAM 정책을 구성할 수 있습니다. | 2020년 9월 10일 |
| 구성원 계정에 대한 BatchUpdateFindings 의 액세스 확대 | 이제 기본적으로 멤버 계정은 관리자 계정과 동일하게 BatchUpdateFindings 에 대한 액세스 권한을 가집니다. | 2020년 9월 10일 |
| 기본 보안 모범 사례 표준 AWS KMS 의에 대한 새로운 제어 | Foundational Security Best Practices 표준에 두 가지 새로운 제어(KMS.1 및 KMS.2)를 추가했습니다. 새로운 제어는 IAM 정책이 AWS KMS 복호화 작업에 대한 액세스를 제한하는지 여부를 확인합니다. | 2020년 9월 9일 |

| | | |
|---|---|---|
| 제어에 대한 계정 수준의 조사 결과 삭제 | Security Hub CSPM은 더 이상 제어에 대한 계정 수준의 조사 결과를 생성하지 않습니다. 리소스 수준 조사 결과만 생성됩니다. | 2020년 9월 1일 |
| ASFF에서 새로운 PatchSummary 객체 | `PatchSummary` 객체를 ASFF에 추가했습니다. `PatchSummary` 객체는 선택한 규정 준수 표준과 관련된 리소스의 패치 규정 준수에 대한 정보를 제공합니다. | 2020년 9월 1일 |
| 새롭게 디자인된 제어 세부 정보 페이지 | 제어의 세부 정보 페이지가 새롭게 디자인되었습니다. 제어 조사 결과 목록은 규정 준수 상태를 기반으로 목록을 빠르게 필터링할 수 있는 탭을 제공합니다. 또한 숨겨진 조사 결과를 빠르게 확인할 수 있습니다. 각 항목은 조사 결과 리소스, AWS Config 규칙 및 조사 결과 노트에 대한 추가 세부 정보에 대한 액세스를 제공합니다. | 2020년 8월 28일 |
| 조사 결과에 대한 새로운 필터 옵션 | 조사 결과 필터의 경우, is not 필터를 사용하여 필드 값이 필터 값과 같지 않은 조사 결과를 찾을 수 있습니다. does not start with를 사용하여 필드 값이 지정된 필터 값으로 시작하지 않는 조사 결과를 찾을 수 있습니다. | 2020년 8월 28일 |

| | | |
|---|---|---|
| ASFF에서 새로운 리소스 세부 정보 객체 | `AwsDynamoDbTable` , `AwsEc2Eip` , `AwsIamPolicy` , `AwsIamUser` , `AwsRdsDbCluster` , `AwsRdsDbClusterSnapshot` , `AwsRdsDbSnapshot` , `AwsSecretsManagerSecret` 리소스 유형에 대해 새로운 `Resources.Details` 객체 추가 | 2020년 8월 18일 |
| RSA Archer와의 새로운 통합 | 이제 Security Hub CSPM은 RSA Archer와 통합됩니다. RSA Archer는 Security Hub CSPM으로부터 조사 결과를 수신합니다. | 2020년 8월 18일 |
| AWSKmskey에 대한 새로운 설명 필드 | `Resources.Details` 에 있는 `AwsKmsKey` 객체에 `Description` 필드를 추가했습니다. | 2020년 8월 18일 |
| AwsRdsDbInstance에 필드 추가 | `Resources.Details` 에 있는 `AwsRdsDbInstance` 객체에 몇 가지 속성을 추가했습니다. | 2020년 8월 18일 |
| Security Hub CSPM이 제어의 전체 상태를 결정하는 방법 업데이트 | 조사 결과가 없는 제어의 경우, 상태는 알 수 없음 대신 데이터 없음입니다. 제어 상태에는 계정 수준 및 리소스 수준 조사 결과가 모두 포함됩니다. 제어 상태는 숨겨진 조사 결과를 무시하는 경우를 제외하고는 조사 결과의 워크플로우 상태를 사용하지 않습니다. | 2020년 8월 13일 |

| | | |
|---|---|---|
| Security Hub CSPM이 표준에 대한 보안 점수를 계산하는 방식 업데이트 | 이제 Security Hub CSPM이 표준에 대한 보안 점수를 계산할 때 데이터 없음 상태인 제어를 무시합니다. 보안 점수는 데이터가 없는 제어를 제외하고, 통과된 제어와 활성화된 제어의 비율입니다. | 2020년 8월 13일 |
| 활성화된 표준에서 새로운 제어를 자동으로 활성화하는 새로운 옵션 | 활성화된 표준에서 새로운 제어를 자동으로 활성화하는 설정 옵션이 추가되었습니다. `UpdateSecurityHubConfiguration` API 작업을 사용하여 이 옵션을 구성할 수도 있습니다. | 2020년 7월 31일 |
| PCI DSS(지불 카드 산업 데이터 보안 표준)에 대한 새로운 컨트롤 | PCI DSS 표준에 새로운 제어를 추가했습니다. 새로운 제어의 식별자는 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, PCI.SSM.3입니다. | 2020년 7월 29일 |
| Foundational Security Best Practices 표준에 대한 새로운 및 업데이트된 제어 | Foundational Security Best Practices 표준에 새로운 제어 추가 새로운 제어의 식별자는 AutoScaling.1, DMS.1, EC2.4, EC2.6, S3.5, SSM.3입니다. ACM.1의 제목을 업데이트하고 `daysToExpiration` 파라미터 값을 30으로 변경했습니다. | 2020년 7월 29일 |

| | | |
|---|---|---|
| ASFF에서 새로운 Vulnerabilities 객체 | 조사 결과와 관련된 취약성에 대한 정보를 제공하는 Vulnerabilities 객체가 추가되었습니다. | 2020년 7월 1일 |
| Auto Scaling 그룹, EC2 볼륨 및 EC2 VPC에 대한 ASFF의 새로운 Resource.Details 객체 | Resource.Details 에 AwsAutoScalingAutoScalingGroup , AWSEc2Volume 및 AwsEc2Vpc 객체가 추가되었습니다. | 2020년 7월 1일 |
| ASFF에서 새로운 NetworkPath 객체 | 조사 결과와 관련된 네트워크 경로에 대한 정보를 제공하는 NetworkPath 객체가 추가되었습니다. | 2020년 7월 1일 |
| Compliance.Status 이(가) PASSED인 경우, 조사 결과를 자동으로 해결합니다 | 제어의 조사 결과의 경우, Compliance.Status 가 PASSED이면 Security Hub CSPM은 자동으로 Workflow.Status 을(를) RESOLVED로 설정합니다. | 2020년 6월 24일 |
| AWS Command Line Interface 예제 | 여러 Security Hub CSPM 작업에 대한 AWS CLI 구문과 예제가 추가되었습니다. Security Hub CSPM 활성화, 인사이트 관리, 표준 및 제어 관리, 제품 통합 관리, Security Hub CSPM 비활성화가 포함됩니다. | 2020년 6월 24일 |

| | | |
|---|---|---|
| ASFF의 새로운 Severity.Original 속성 | 조사 결과 공급자의 원래 심각도인 Severity.Original 속성을 추가했습니다. 이는 더 이상 사용되지 않는 Severity.Product 속성을 대체합니다. | 2020년 5월 20일 |
| 컨트롤 상태에 대한 세부 정보를 제공하는 ASFF의 새로운 Compliance.StatusReasons 객체 | 제어의 현재 상태에 대한 추가 컨텍스트를 제공하는 Compliance.StatusReasons 객체를 추가했습니다. | 2020년 5월 20일 |
| 새로운 AWS 기본 보안 모범 사례 표준 | 배포된 계정 및 리소스가 보안 모범 사례에서 벗어나는 시점을 감지하는 제어 세트인 새로운 AWS 기본 보안 모범 사례 표준이 추가되었습니다. | 2020년 4월 22일 |
| 조사 결과에 대한 워크플로우 상태를 업데이트하는 새로운 콘솔 옵션 | Security Hub 콘솔 또는 API를 사용하여 조사 결과의 워크플로우 상태를 설정하는 데 필요한 정보가 추가되었습니다. | 2020년 4월 16일 |
| 조사 결과에 대한 고객 업데이트를 위한 새로운 BatchUpdateFindings API | 조사 결과 조사 프로세스와 관련된 정보를 업데이트하기 위해 BatchUpdateFindings 을(를) 사용하는 방법에 대한 정보가 추가되었습니다. BatchUpdateFindings 이(가) UpdateFindings (으)로 대체되며, 이는 더 이상 사용되지 않습니다. | 2020년 4월 16일 |

| | | |
|---|---|---|
| AWS Security Finding 형식 (ASFF) 업데이트 | 여러 가지 새로운 리소스 유형이 추가되었습니다. `Severity` 객체에 새로운 `Label` 속성이 추가되었습니다. `Label`은 `Normalized` 필드를 대체하기 위한 것입니다. 조사 결과 조사 과정을 추적하기 위해 새로운 `Workflow` 객체가 추가되었습니다. `Workflow`에는 기존 `Workflowstate` 속성을 대체하는 `Status` 속성이 포함되어 있습니다. | 2020년 3월 12일 |
| 통합 페이지에 대한 업데이트 | 통합 페이지에 변경 사항을 반영하도록 업데이트되었습니다. 이제 각 통합에 대해 페이지에 통합 범주가 표시되고 각 통합에서 Security Hub CSPM의 조사 결과를 전송 또는 수신하는지 여부가 표시됩니다. 또한 각 통합을 활성화하는 데 필요한 특정 단계를 제공합니다. | 2020년 2월 26일 |
| 새로운 타사 제품 통합 | 새로운 제품 통합인 Cloud Custodian, FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security 및 Vectra.ai Cognito Detect가 추가되었습니다. | 2020년 2월 21일 |

| | | |
|---|---|---|
| PCI DSS(지불 카드 산업 데이터 보안 표준)에 대한 새로운 보안 표준 | PCI DSS(지불 카드 산업 데이터 보안 표준)에 대한 Security Hub CSPM 보안 표준이 추가되었습니다. 이 표준이 활성화되면 Security Hub CSPM은 PCI DSS 요구 사항과 관련된 제어에 대해 자동화된 확인을 수행합니다. | 2020년 2월 13일 |
| AWS Security Finding 형식(ASFF) 업데이트 | 표준 제어의 관련 요구 사항에 대한 필드가 추가되었습니다. 새로운 리소스 유형 및 새로운 리소스 세부 정보가 추가되었습니다. 또한 ASFF를 사용하면 이제 최대 32개의 리소스를 제공할 수 있습니다. | 2020년 2월 5일 |
| 개별 보안 표준 제어를 비활성화하는 새로운 옵션 | 각 개별 보안 표준 제어가 활성화되는지 여부를 제어하는 방법에 대한 정보가 추가되었습니다. | 2020년 1월 15일 |
| Security Hub CSPM 개념 업데이트 | Security Hub CSPM 개념에 일부 설명이 업데이트되었고 새로운 용어가 추가되었습니다. | 2019년 9월 21일 |
| AWS Security Hub CSPM 정식 출시 | 프리뷰 기간 동안 Security Hub CSPM의 개선 사항을 반영하여 콘텐츠가 업데이트되었습니다. | 2019년 6월 25일 |
| CIS AWS Foundations 검사에 대한 수정 단계 추가 | AWS Security Hub CSPM에서 지원되는 보안 표준에 문제 해결 단계를 추가했습니다. | 2019년 4월 15일 |
| AWS Security Hub CSPM의 베타 릴리스 | AWS Security Hub CSPM 사용 설명서의 베타 릴리스 버전이 게시되었습니다. | 2018년 11월 18일 |

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.