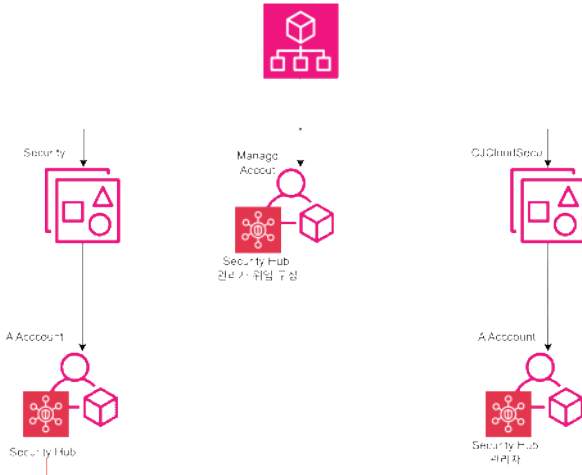


Security Hub 이벤트 통합방안

2025년 12월 11일 목요일 오전 10:56

1. 구성 목표

Security Hub 관리자 대시보드에서 위임 받은 타 계정의 보안 서비스 이벤트 통합



2. 위임 설정

- a. Organization 관리계정에서 Security hub 위임설정 #AWS 계정에 Security Hub 관리계정 입력

Security Hub 구성

이렇게 하면 **서비스 연결 역할(SLR)**을 생성할 수 있는 권한이 부여되고 Security Hub의 **이용 약관**에 동의하게 됩니다.

위임된 관리자 계정

이렇게 하면 선택한 계정이 Security Hub, Security Hub CSPM, GuardDuty 및 Inspector의 위임 관리자로 지정됩니다. 이미 이러한 서비스 중 하나에 위임 관리자를 지정한 경우 해당 서비스의 위임 관리자는 업데이트되거나 변경되지 않습니다.

신뢰할 수 있는 액세스

☒ 위임된 관리자에 대한 신뢰할 수 있는 액세스 권한을 부여합니다.

이를 통해 위임받은 관리자는 멤버 계정에 액세스도 방지 기능과 같은 특정 기능을 구성할 수 있는 권한을 갖게 됩니다.

AWS 계정

962889423329

계정 ID는 12자리 숫자여야 합니다.

위임 관리자 정책

이 정책 설정은 구성 정책 생성을 포함한 Security Hub 관리 권한을 위임 관리자에게 부여합니다.

☒ 위임 정책은 필요한 모든 정책 조항을 포함하여 최신 상태로 유지됩니다. 위임받은 관리자는 정책을 완벽하게 관리할 수 있습니다.

▼ 정책 세부 정보

```
61 }
62 },
63 {
64   "Sid": "SecurityServicesDelegatingPolicy#MutationActions",
65   "Effect": "Allow",
```

새로운 보안 허브의 가격 정보

Security Hub의 가격 정책은 리소스별 기본 요금이 부과되는 필수 기능, 별도 요금이 부과되는 위험 분석 기능, 그리고 추가 기능(역시 별도 요금 부과)으로 구성됩니다.

[예상 견적 보기 >](#)

▼ 보안 허브의 핵심 기능

| 보안 허브 | 자원별 가격 책정 |
|--------------------------------------|---|
| 노출 상관관계, 자원 목록, 결과 집계 및 워크플로 자동화 | EC2 인스턴스, ECR 컨테이너 이미지, 람다 함수, IAM 사용자 및 IAM 역할 |
| 보안 허브 CSPM CSPM 검사 | |
| 경비 업무 | |
| EC2 자동 액세스코드 검사 | |
| 검사기 | |
| EC2 스케닝, ECR 스케닝, 람다 표준 스캐닝, CIS 스캐닝 | |

① 핵심 기능 30일 무료 체험

Security Hub의 30일 무료 체험 기간 동안에는 필수 기능에 대한 비용을 30일 동안 지불하지 않아도 됩니다.

- b. 위임 정책 생성 #Organization 관리계정에서 Security Hub 접속 시 자동으로 표시
- c. Security Hub 관리계정 접속 후 조직 구성

Security Hub

대시보드

요약
위험
노출
취약성
상태 관리
민감한 데이터
인벤토리
All findings
리소스

▼ 관리

구성
자동화
통합

구성 정보

Configure security capabilities across your organization by selecting policies or deployments from the Catalog tab. Policies and deployments define how capabilities are configured across accounts and Regions. Unlike policies, a deployment is a one-time action. To review coverage details for accounts in your organization, go to [Account Coverage](#).

Configured policies | Configuration catalog

정책

정책을 통해 조직 전체의 구성을 관리할 수 있습니다. 또한 [AWS Organizations](#)에서 정책을 보고 관리할 수 있습니다.

Q 정책 이름 또는 정책 유형별 필터링

| 정책 이름 | 정책 유형 |
|-------|-------|
| | |

정책 없음

[구성](#)

정책 [삭제](#) [편집](#) [구성](#)

계정 범위 및 리전 선택 #특정 계정 및 서울 리전에만 활성화하도록 구성함

Security Hub CSPM > 분석 결과

모락

제어

보안 표준

인사이드

분석 결과

통합

▼ 관리

자동화

사용자 지정 작업

▼ 설정

일반

리전

구성 관리

사용량

세로운 소식

Security Hub Advanced

분석 결과

조사 결과는 보안 문제 또는 실재한 보안 인시던트다. 그룹화 기준을 선택한 다음 인시던트를 생성하여 관련 조사 결과를 저장할 수 있습니다.

Findings might be inaccurate
If you receive a failed finding for Config 1, you might not have AWS Config recording correctly configured. This can result in inaccurate control findings.

Learn more about AWS Config setup

Q. 필터 추가

레전드 상태 분석결과 ACTIVE

필터 적용하기

제출 이름

개수

Prisma Cloud Compute

1557

Security Hub

820

GuardDuty

764

그룹화 기준

제출 이름

분석 결과 (20+)

조사 결과는 보안 문제 또는 실재한 보안 인시던트다. 그룹화 기준을 선택한 다음 인시던트를 생성하여 관련 조사 결과를 저장할 수 있습니다.

Findings might be inaccurate
If you receive a failed finding for Config 1, you might not have AWS Config recording correctly configured. This can result in inaccurate control findings.

Learn more about AWS Config setup

Q. 필터 추가

레전드 상태 분석결과 ACTIVE

필터 적용하기

| 조사 결과 | 실적도 | 위조물류 상태 | 리전 | 계정 ID | 회사 | 제품 | 리소스 | 공통 준수 상태 | 업데이트 시간 |
|---|-----|----------|----------------|--------------|--------------------|----------------------|---|----------|---------|
| Host runtime anomaly | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 753 dslp-n-prd-ecs-vm-1 | 24시간 전 | |
| Host runtime anomaly | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 753 ip-10-85-96-139.ap-northeast-2-compute-internal | 24시간 전 | |
| Host runtime anomaly | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 753 Pccnode2 | 24시간 전 | |
| Container runtime anomaly - Suspicious network activity - Suspicious network activity | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 254014 ecs-pp-apr8-prd-Rout8-app-task-47-gg-app8-front-app-44258a69b079819601 | 24시간 전 | |
| Host runtime anomaly | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 753 Ppr-prd-ecs-vm-2 | 24시간 전 | |
| Host runtime anomaly | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 753 Pccnode1 | 24시간 전 | |
| Container runtime anomaly - Dns query - Dns query | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 254014 ecs-k8s-wcs-gg30-prd-w2-ecs-task-batch-1-k8s-wcs-gg30-batch-c8817f9ed8dd676a0300 | 24시간 전 | |
| Container runtime anomaly - Dns query - Dns query | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 254014 ecs-k8s-wcs-rq01-prd-web-task-2-k8s-ecs-rq01-web-58954e64b0c866e5d00 | 24시간 전 | |
| Container runtime anomaly - Dns query - Dns query | NEW | RESOLVED | ap-northeast-2 | 962889425329 | Palo Alto Networks | Prisma Cloud Compute | 254014 ecs-k8s-wcs-rq01-prd-web-task-2-k8s-wcs-rq01-web-fa08f950a3d614a82350 | 24시간 전 | |

Host runtime anomaly

NEW RESOLVED

최종 업데이트: 14:27:02

Log inspection audit for log file: /var/log/amazon/son/amazon-sm-agent.log, line: 2025-12-12 18:00:12.8279 [INFO] [sm-agent worker] [messageReceived] [NGCConnector] Successfully opened websocket connection to: 43.202.72.118:443

작업

| 제출 | 리소스 | 기록 |
|----------|---------------------------------------|----|
| 조사 결과 ID | app-mgmt-vm/1765530567-9 | |
| 부팅 | Unusual Behaviors/Container | |
| 위조물류 상태 | 해결됨 | |
| 레전드 상태 | ACTIVE | |
| 계정 ID | 962889425329 | |
| 제출 이름 | KDO_DEV | |
| 최종 업데이트 | December 12, 2025, 09:09:27 UTC+00:00 | |
| | 자세히 보기 | |

리소스

| 기타 | |
|---------------------|---------------------|
| dslp-n-prd-ecs-vm-1 | |
| 공통 | Other |
| ARN | dslp-n-prd-ecs-vm-1 |

세부 정보 보기

기록

December 12, 2025

10:25:59 UTC+00:00

by [1] Security Hub - AWS

18:00

Workflow Status changed from "NEW" to "RESOLVED"

09:08:28 UTC+00:00

by [1] Security Hub - AWS

18:00

조사 결과 생성됨

세부 정보 보기

4. 후속 과제

- a. 이벤트 알림 발생: Lambda 또는 Step Function 적용해서 심각도 기준, Teams 알림 발생
- b. 증적 저장: JIRA 연동해서 Lois Servin 내 티켓팅 생성

업무 페이지 3