AWSKRUG

Security Hub

어디까지 써봤니?

Daegon Kim

Cloud Architect,
AWS Professional Services

Today’s Speaker

김대곤
Cloud Architect
AWS Professional Services

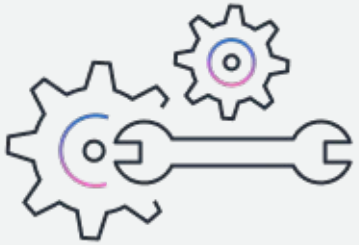
- 미국에서 PHP 서버 개발을 하며 DevOps에 관심을 가지게 됨
- 현재 Proserve 팀에서 DevOps 관련 업무를 주로 담당하고 있습니다.
- Agile, Container, DevSecOps 및 CloudOps에 관심이 많습니다.

Agenda

- Security and compliance challenges
- Security Hub Overview
- Security Hub Use Case

Security and compliance challenges

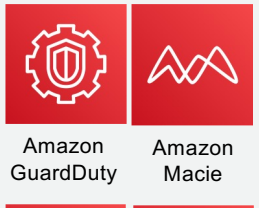
Lack of visibility into security risks

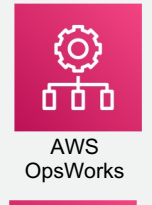


Complexity of tools, vendors, and processes

Too many alerts, and not enough security experts

AWS Foundational and Layered Security Services

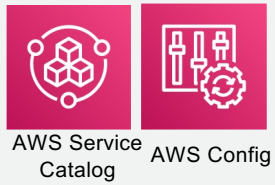


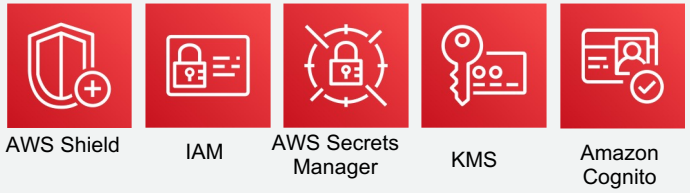


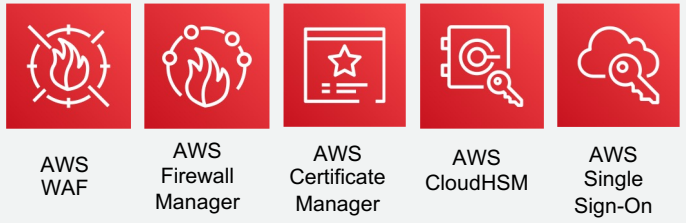
Identify → Protect → Detect → Respond → Recover

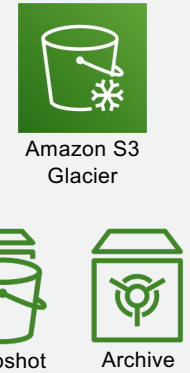
Automate

Investigate



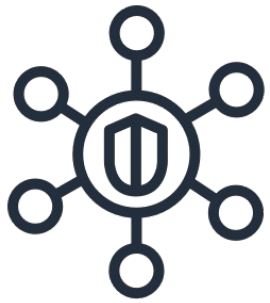




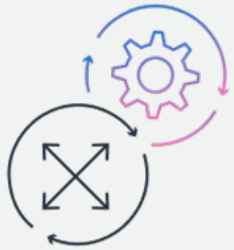


Security Hub Overview

What is AWS Security Hub?



AWS Security Hub는 보안 모범 사례 점검을 **지속적**으로 수행하고 AWS 및 타사 서비스의 보안 결과를 **원활하게** 집계하여 자동화된 대응을 가능하게 하는 클라우드 보안 태세 관리 서비스(CSPM)



자동화된 지속적인 모범 사례 점검

AWS 서비스 및 파트너 서비스 검사 결과와 통합

표준화된 결과 형식 및 교차 리전 간 집계

규제 및 특정 프레임워크에 부합하는 보안 표준 제공

자동화된 대응, 수정 및 강화 조치

Security Hub information flows

Findings ingestions

AWS Config

Amazon GuardDuty

Amazon Inspector

AWS IAM

Amazon Macie

AWS Firewall Manager

CROWDSTRIKE

...and many more

Standards and controls

PCI DSS

NIST

AWS FSBP

CIS AWS Foundations Benchmark

Service-managed standards

AWS Security Hub

Amazon EventBridge

Findings integrations

Amazon Detective

AWS Audit Manager

Security Lake

AWS Trusted Advisor

AWS Chatbot

Remediation actions

AWS Lambda

AWS Systems Manager

AWS Step Functions

Take action with partners

...plus many others

Security Hub

Security Hub

보안과 관련된 통합된 뷰

- AWS Security Hub는 사용자 환경에서 활성화된 AWS 보안 서비스에서 분석 결과를 수집하고 통합

지속적 보안 검사

- 업계 표준 및 모범 사례를 사용하여 계정 및 리소스 수준의 지속적 구성/보안 검사를 자동화

사용자 지정 응답 수신 및 수정 작업

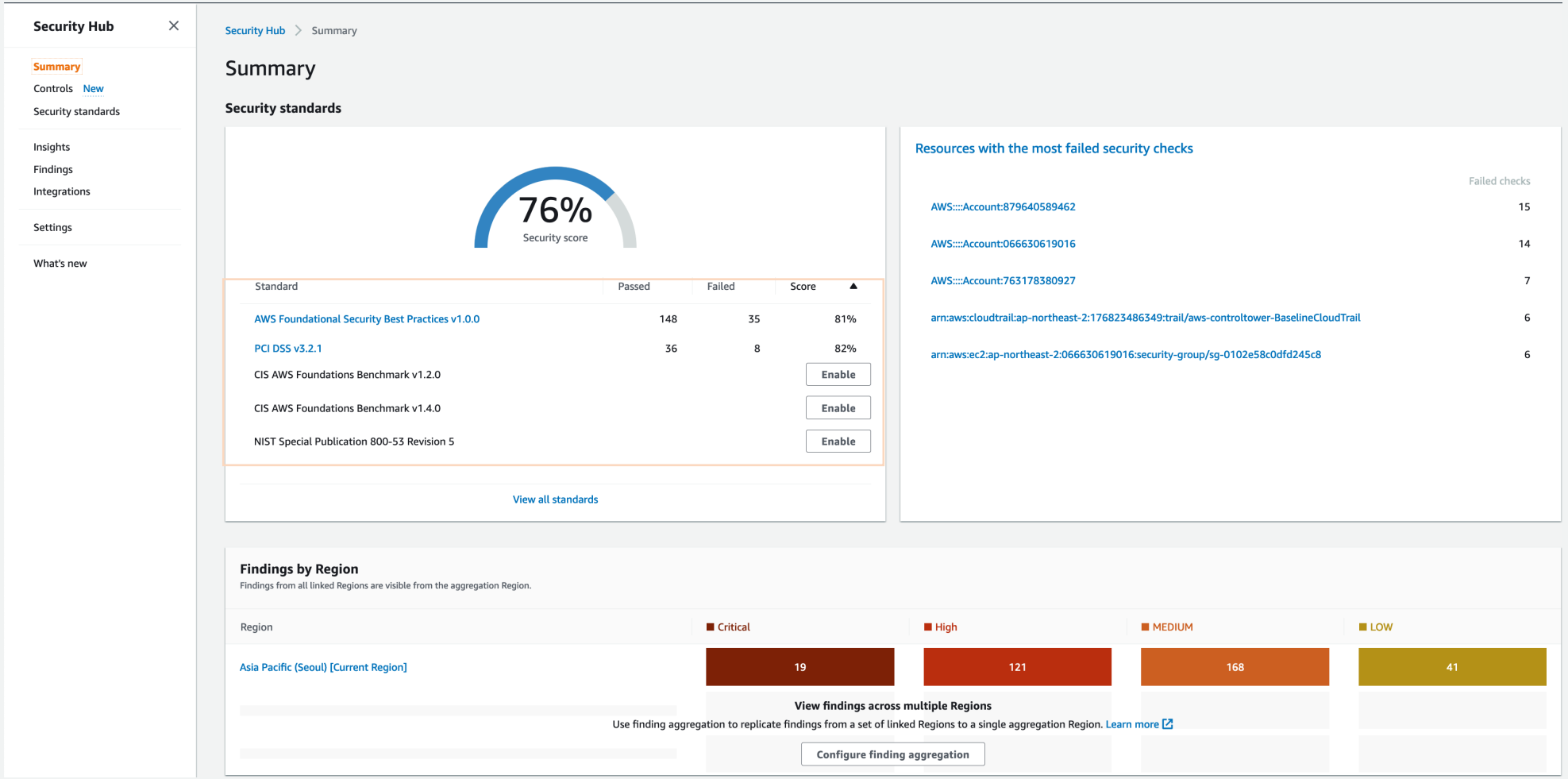
- AWS Security Hub는 Amazon CloudWatch Events와 통합되어, 사용자는 사용자 지정 응답 및 수정 워크플로우를 생성

다중 계정 지원

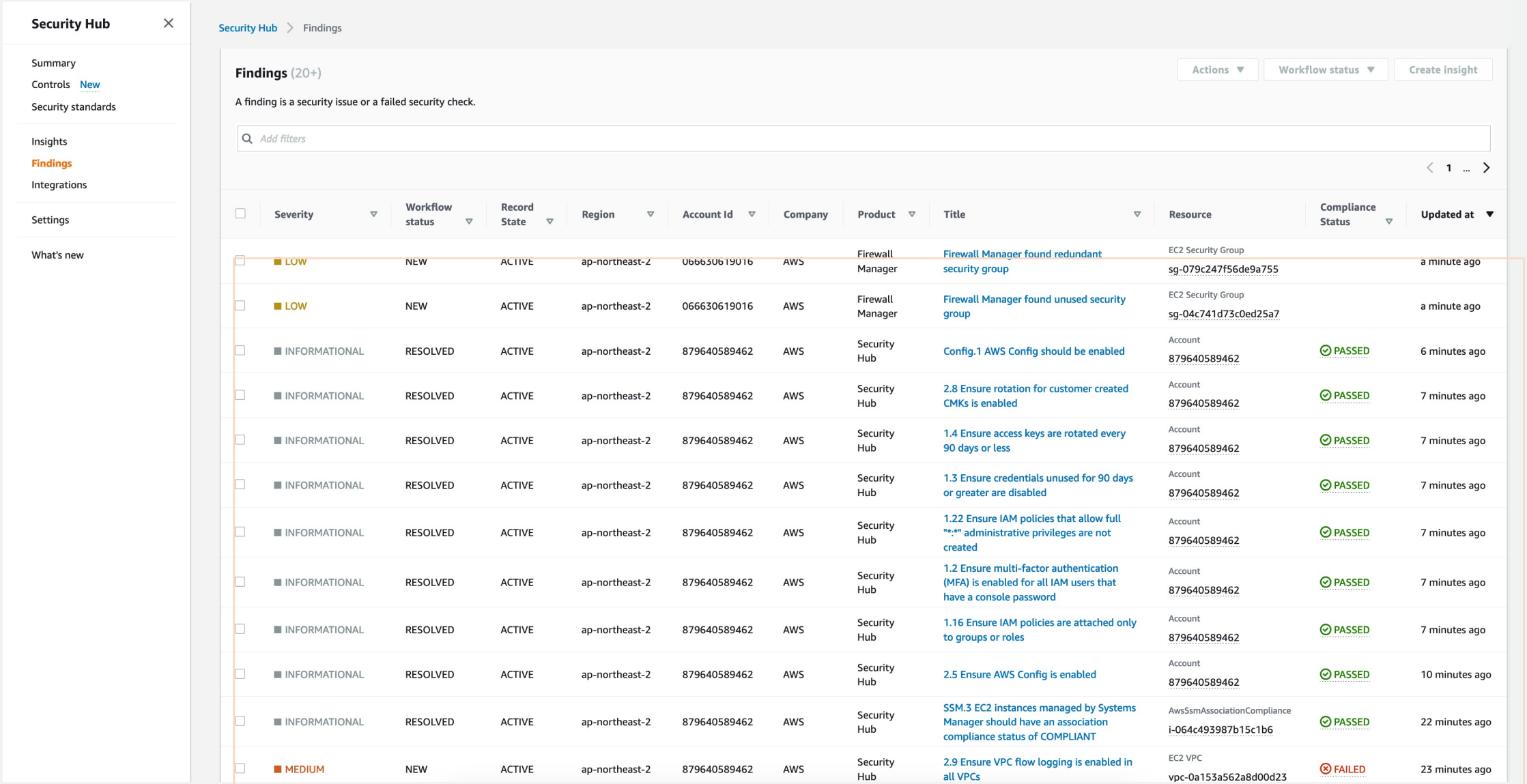
- AWS Security Hub 콘솔에서 몇 번만 클릭하면 여러 AWS 계정을 연결하고 이러한 계정에서 분석 결과를 통합

Security Hub 보안기준 (Security Standards) 검사

- 클라우드 보안 태세 관리(CSPM) 수행 : 전문가가 큐레이팅한 보안 제어 모음을 기반으로 한 자동화된 검사로 위험을 줄이고 CIS, PCI DSS 등과 같은 일반적인 프레임워크에 대한 기본 매핑 기능으로 규정 준수 관리를 간소화

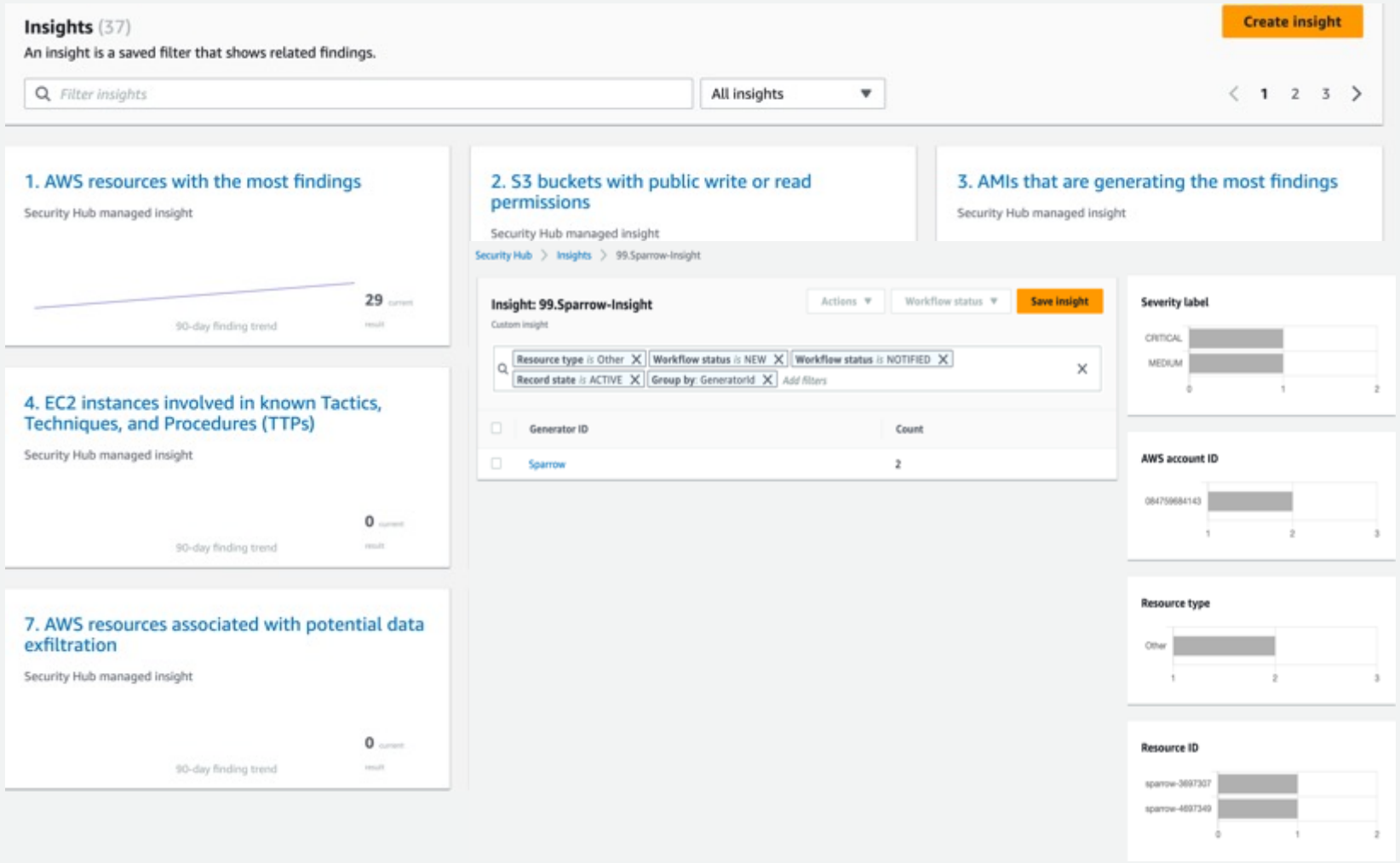


Security Hub Finding(결과) 집계



Security Hub Insights

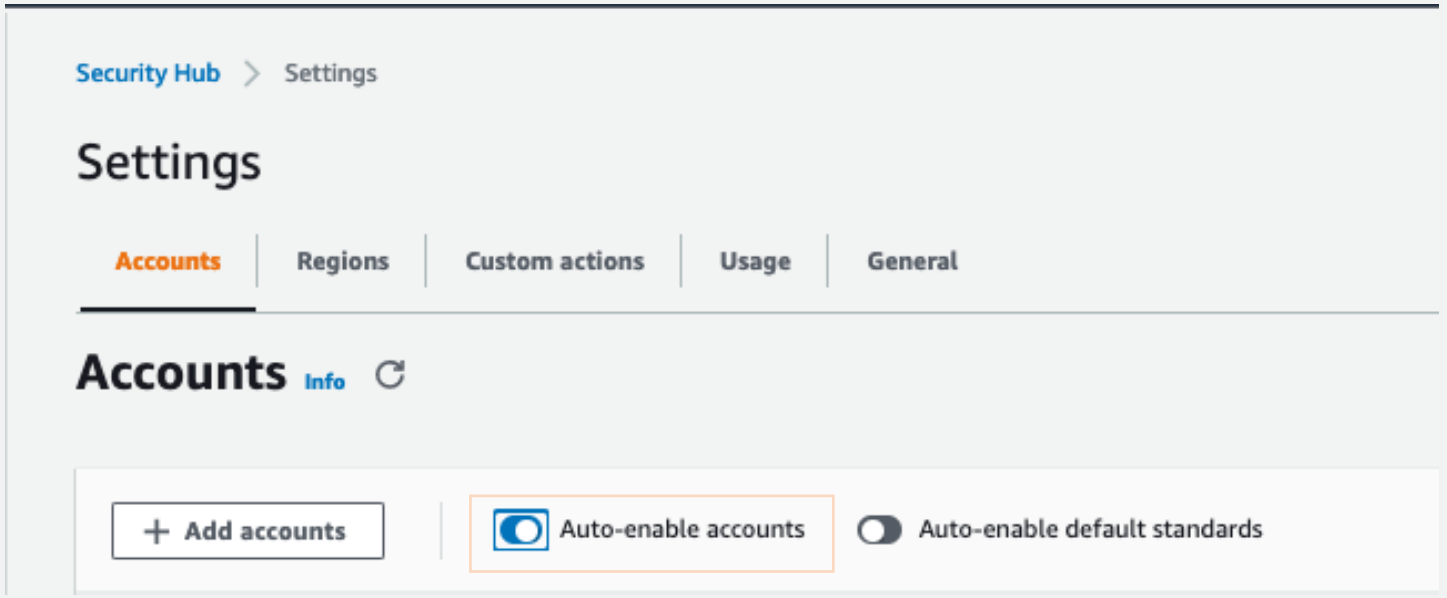
- 주의가 필요한 리소스 및 취약점에 대해 인사이트를 생성하여 관리 가능



- 대시보드를 통해 주요 보안 결과에 대한 가시성 제공
- AWS 및 AWS 파트너가 제공하는 사전 정의된 인사이트 사용 가능
- 커스텀 인사이트를 생성하여 직접 관리 가능

Security Hub 관리 (로그 저장 및 신규 계정에 대한 자동화)

- Security Hub에 쌓인 AWS Native 서비스(GuardDuty, Inspector, Firewall Manager)에 대한 로그는 S3 버킷으로 export하여 저장되며, 보관 주기 정책에 따라 S3 LifeCycle 규칙 적용 (최소 1년 보관)
- Auto-enable Account를 통해 신규 계정 생성시, Security Hub 활성화 및 분석 소스 범위 중 필수에 대해 자동 관리되도록 설계 (선택 분석 로그 적용은 개별 계정 리소스 종류에 따라 수동 관리)



Security Hub 과금 기준

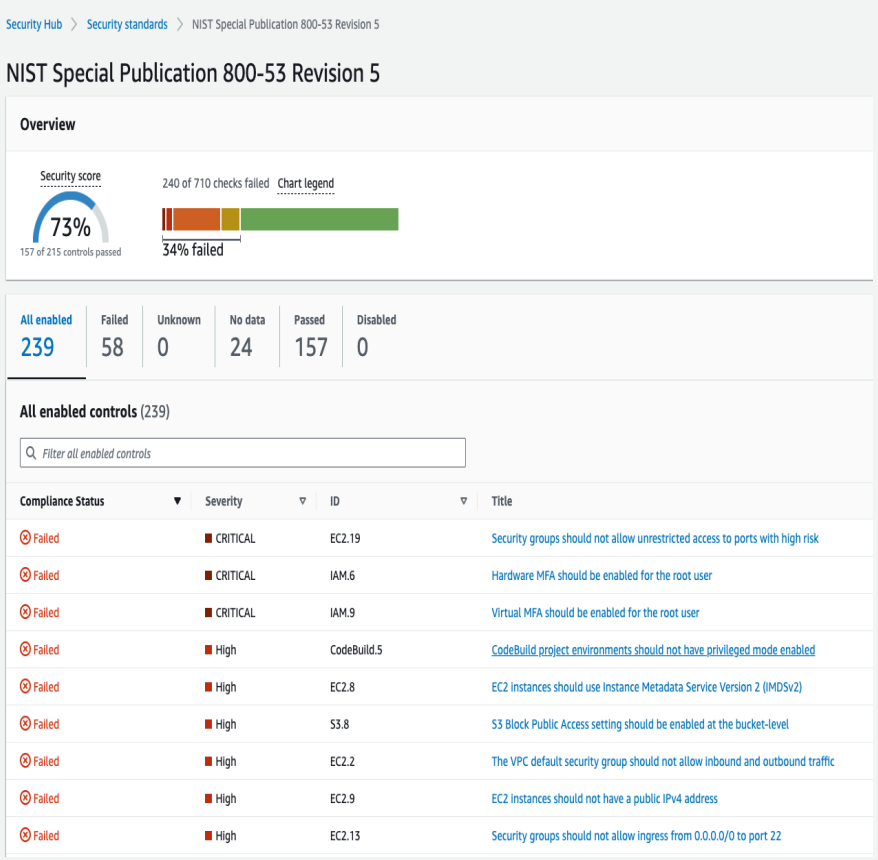
- Security Hub의 과금기준은 아래 2가지 디멘션에 따라 책정됩니다.
- https://aws.amazon.com/ko/security-hub/pricing/

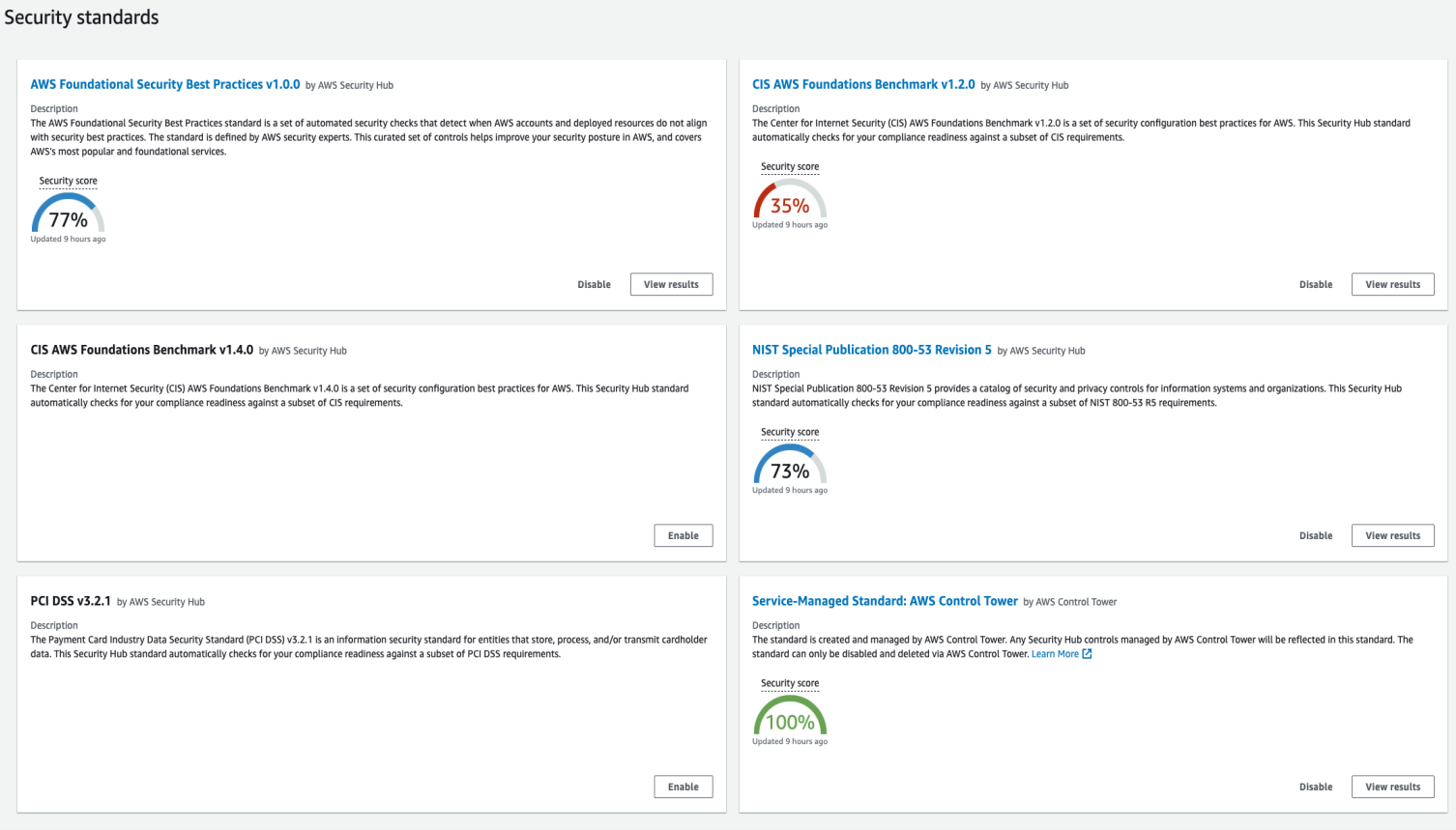
보안기준(Security Standard) 검사	
계정/리전/월당 최초 검사 100,000건	검사당 0.0010 USD
그 이후의 계정/리전/월당 검사 400,000건	검사당 0.0008 USD
계정/리전/월당 검사 500,000건 초과	검사당 0.0005 USD
수집된 Finding(결과)	
Security Hub의 보안 검사와 관련하여 수집된 결과	무료
계정/리전/월당 최초 이벤트 10,000건	무료
계정/리전/월당 최초 이벤트 10,000건 초과	이벤트당 0.00003 USD

Security Hub Use Case

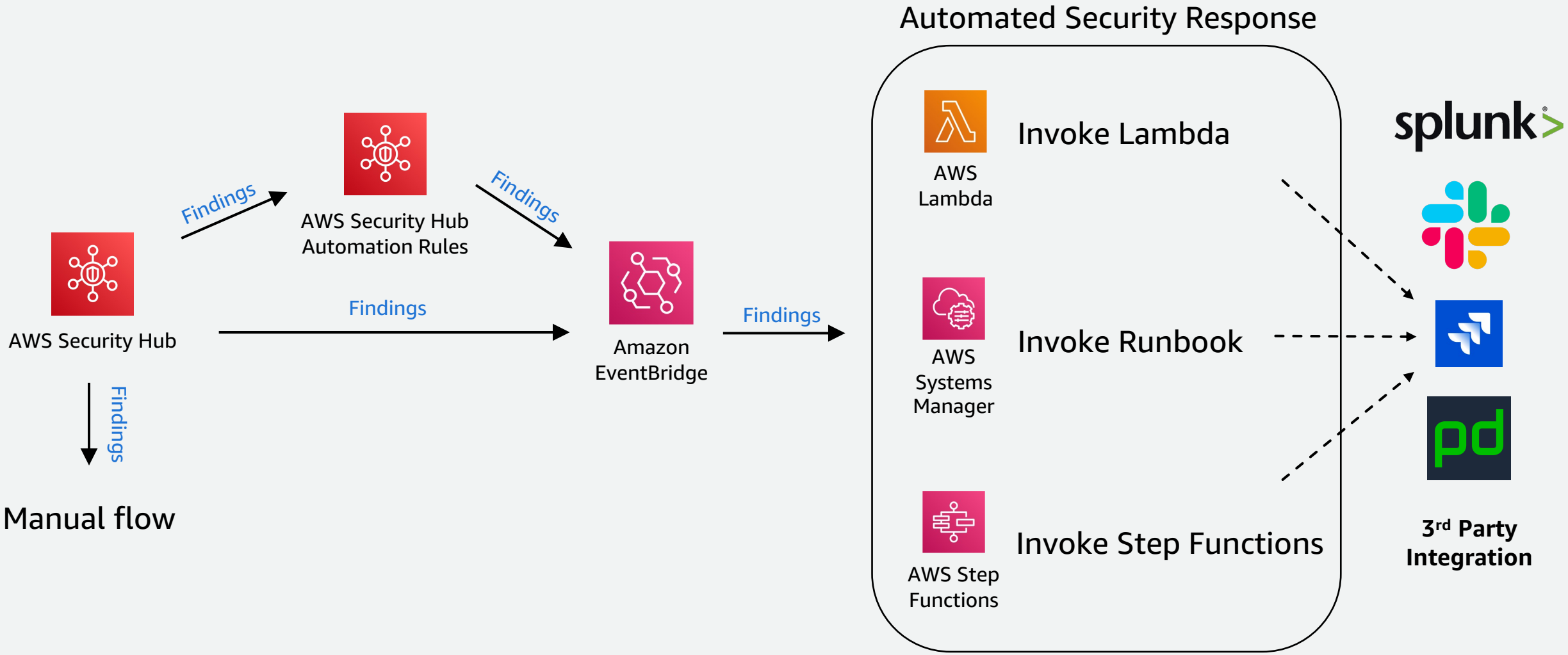
Security Hub Use Case Overview

Posture Management – Use Case



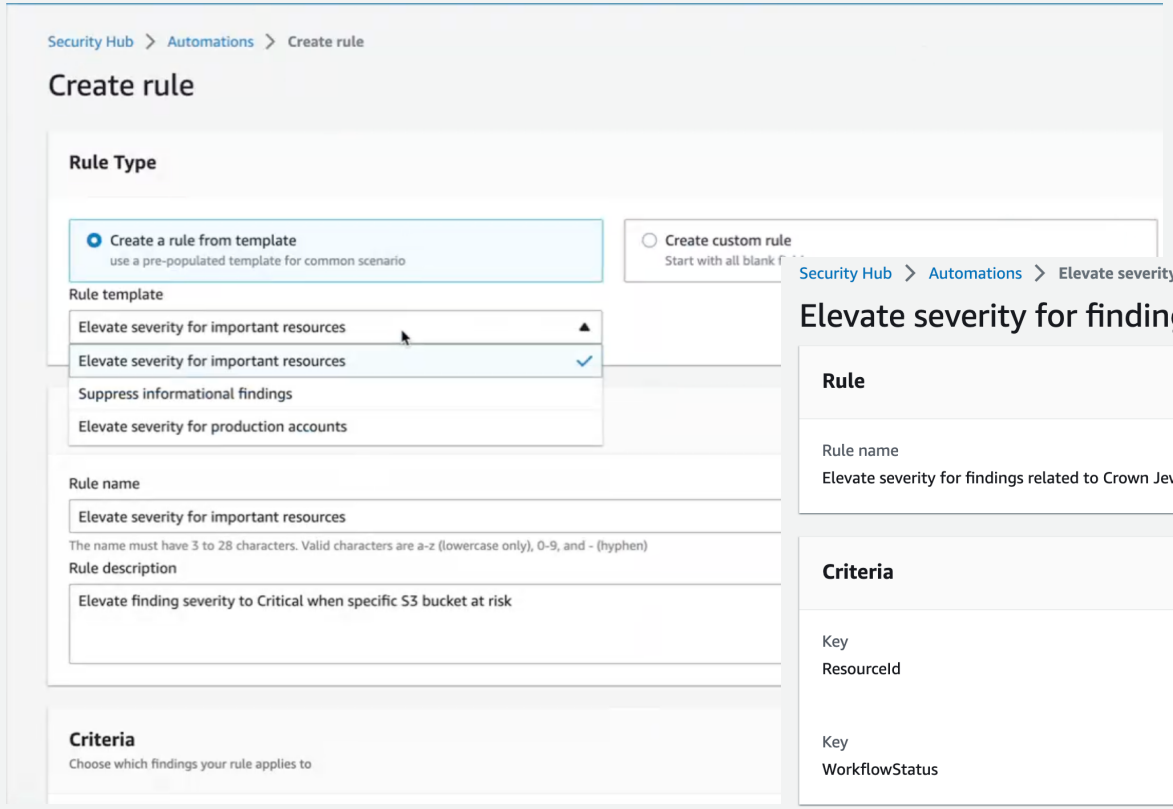


Security Hub Use Case - Automation and Response



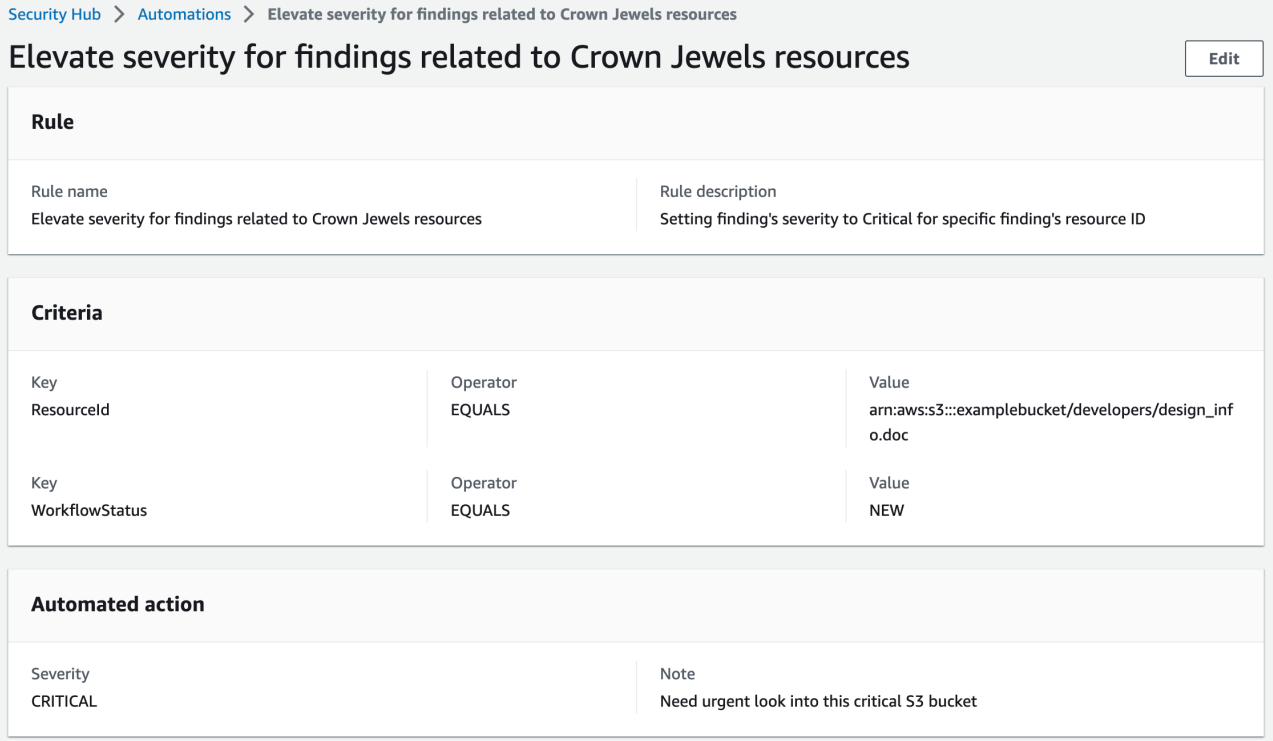
Security Hub Use Case - Automation Rule

자동화 규칙(Automation Rule)을 사용하면 코드 없이도 정의한 기준에 따라 Security Hub 검색 결과를 자동으로 업데이트할 수 있습니다.



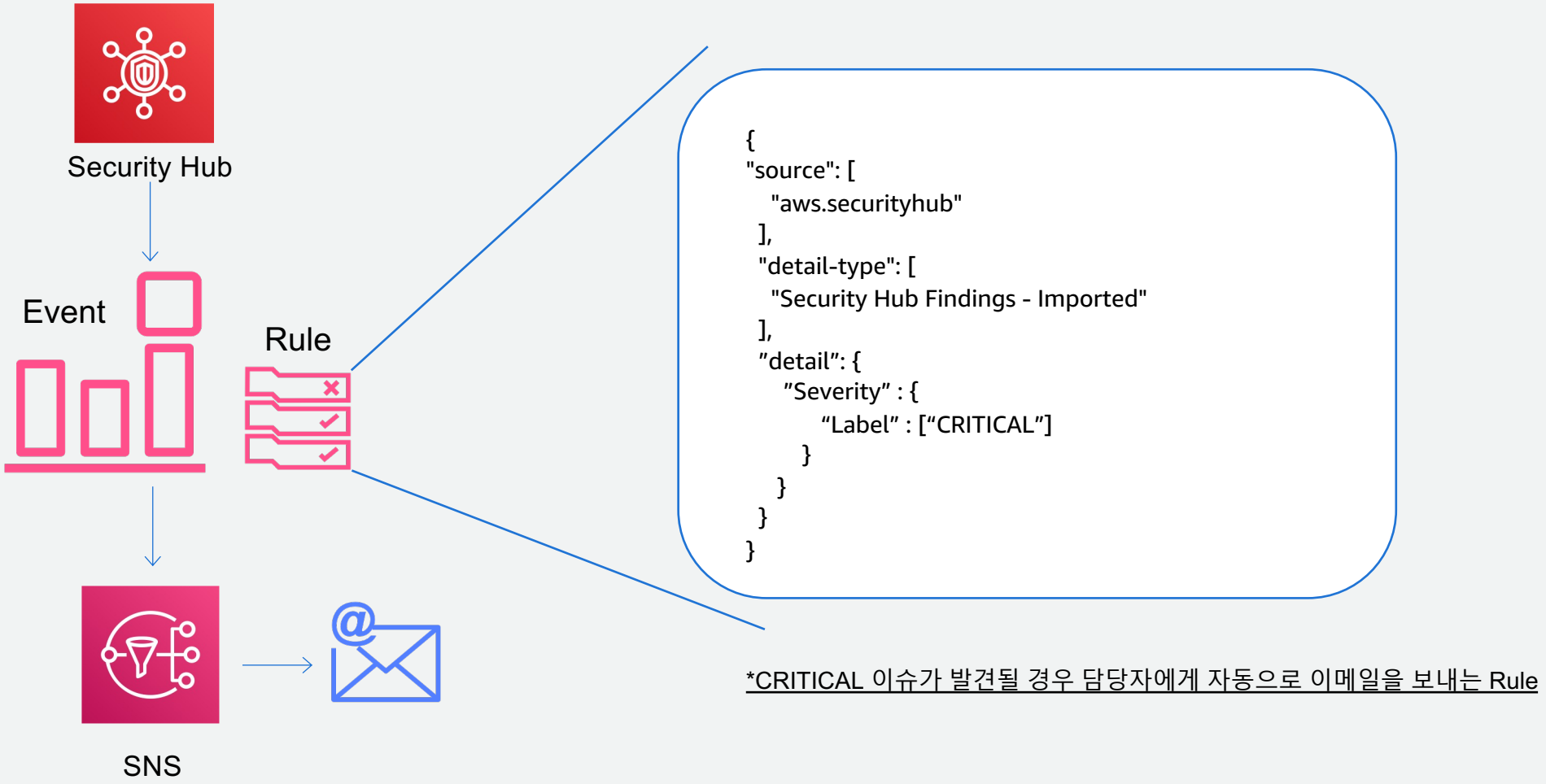
Use cases

- **Changing finding severity**
- **Suppressing findings**
- **Adding notes**



Security Hub Use Case - Automation and Response

- 다른 AWS 서비스와 연계한 자동화 작업 가능



*CRITICAL 이슈가 발견될 경우 담당자에게 자동으로 이메일을 보내는 Rule

Fast and cost saving integration - Use Case

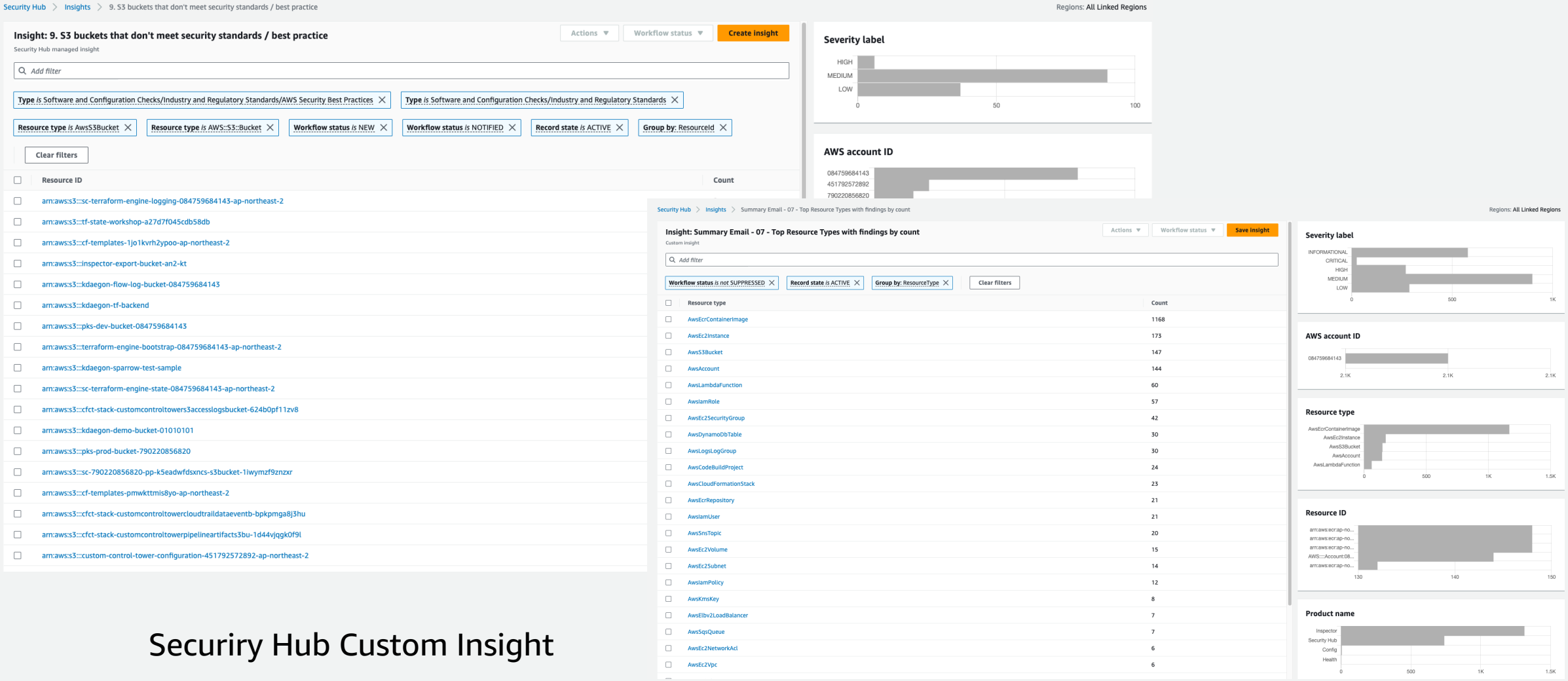
Integrated AWS service	Direction
AWS Config	Sends findings
AWS Firewall Manager	Sends findings
Amazon GuardDuty	Sends findings
AWS Health	Sends findings
AWS Identity and Access Management Access Analyzer	Sends findings
Amazon Inspector	Sends findings
AWS IoT Device Defender	Sends findings
Amazon Macie	Sends findings
AWS Systems Manager Patch Manager	Sends findings
AWS Audit Manager	Receives findings
AWS Chatbot	Receives findings
Amazon Detective	Receives findings
Amazon Security Lake	Receives findings
AWS Systems Manager Explorer and OpsCenter	Receives and updates findings
AWS Trusted Advisor	Receives findings

AWS Native Integration

Integration	Direction
Palo Alto Networks – Prisma Cloud Compute	Sends findings
Palo Alto Networks – Prisma Cloud Enterprise	Sends findings
Prowler – Prowler	Sends findings
Qualys – Vulnerability Management	Sends findings
Rapid7 – InsightVM	Sends findings
SecureCloudDB – SecureCloudDB	Sends findings
SentinelOne – SentinelOne	Sends findings
Snyk	Sends findings
Sonrai Security – Sonrai Dig	Sends findings
Sophos – Server Protection	Sends findings
StackRox – StackRox Kubernetes Security	Sends findings
Sumo Logic – Machine Data Analytics	Sends findings
Symantec – Cloud Workload Protection	Sends findings
Tenable – Tenable.io	Sends findings
Trend Micro – Cloud One	Sends findings
Vectra – Cognito Detect	Sends findings
Wiz	Sends findings
Atlassian - Jira Service Management	Receives and updates findings
Atlassian - Jira Service Management Cloud	Receives and updates findings
Atlassian – Opsgenie	Receives findings
Fortinet – FortiCNP	Receives findings
IBM – QRadar	Receives findings

3rd Party Product Integration

Correlate securiry findings – Use case



Securiry Hub Custom Insight

Demo

Thank you!