



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.

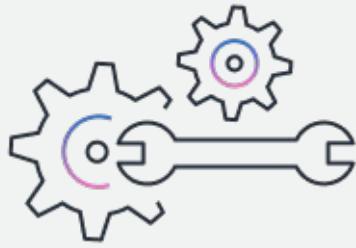
Agenda

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

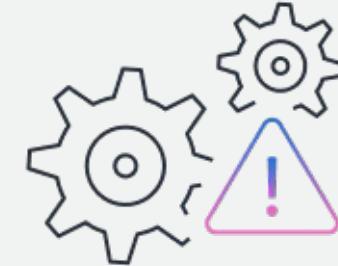
Security and compliance challenges



Lack of visibility into security risks

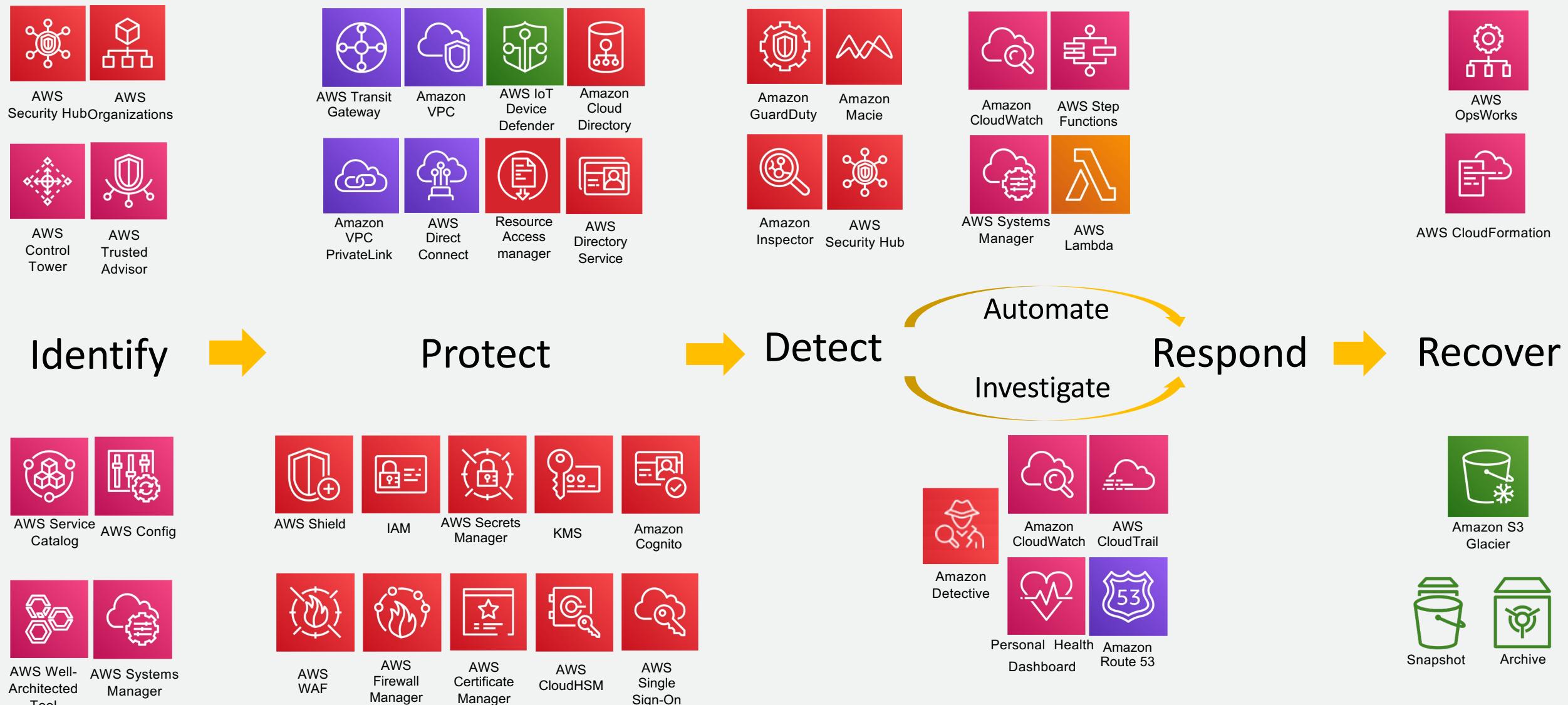


Complexity of tools, vendors, and processes



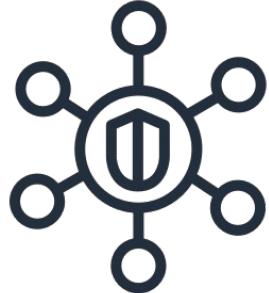
Too many alerts, and not enough security experts

AWS Foundational and Layered Security Services

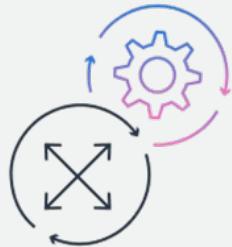


Security Hub Overview

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

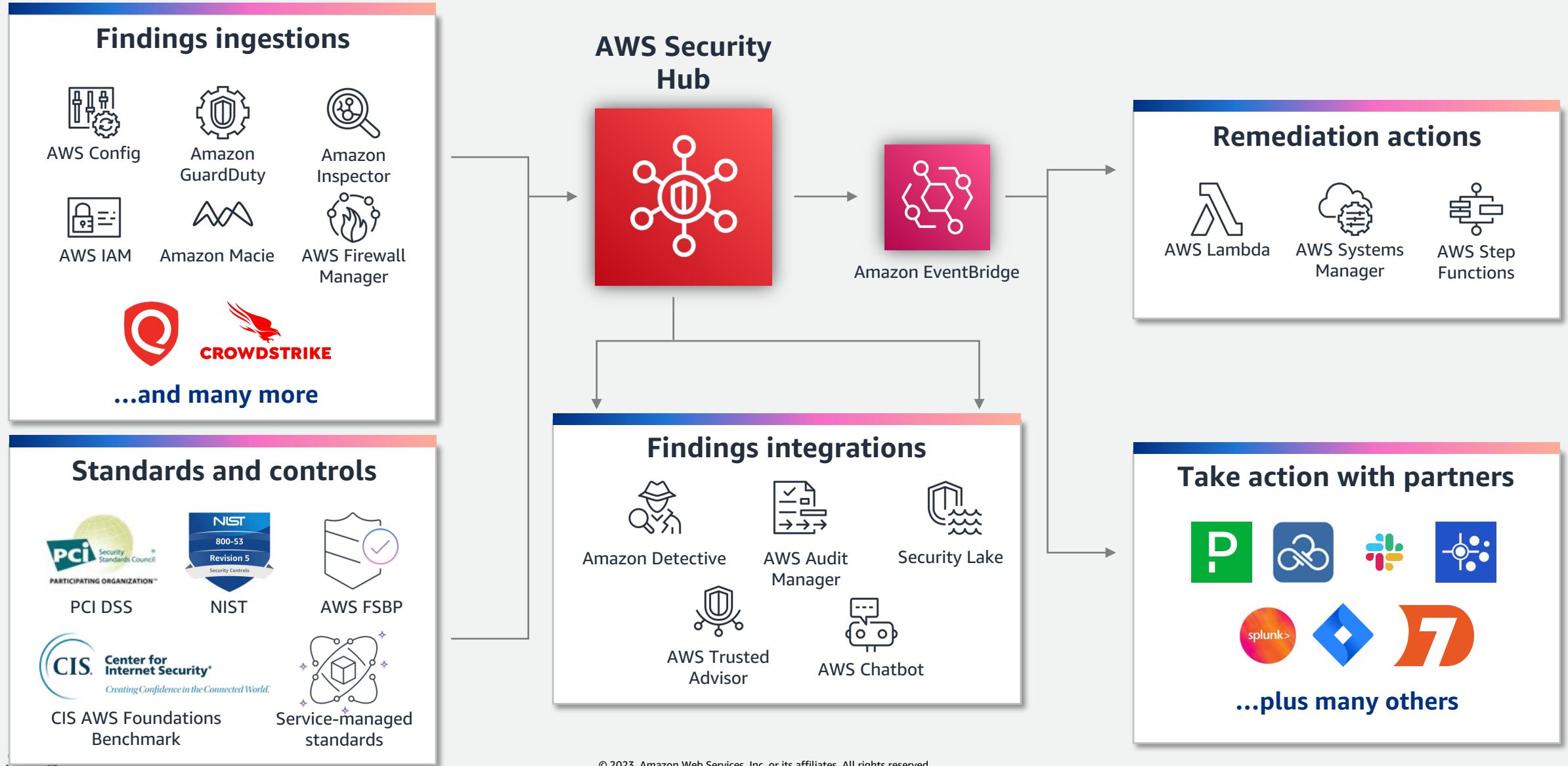


규제 및 특정
프레임워크에
부합하는 보안
표준 제공



자동화된 대응,
수정 및 강화 조치

Security Hub information flows



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

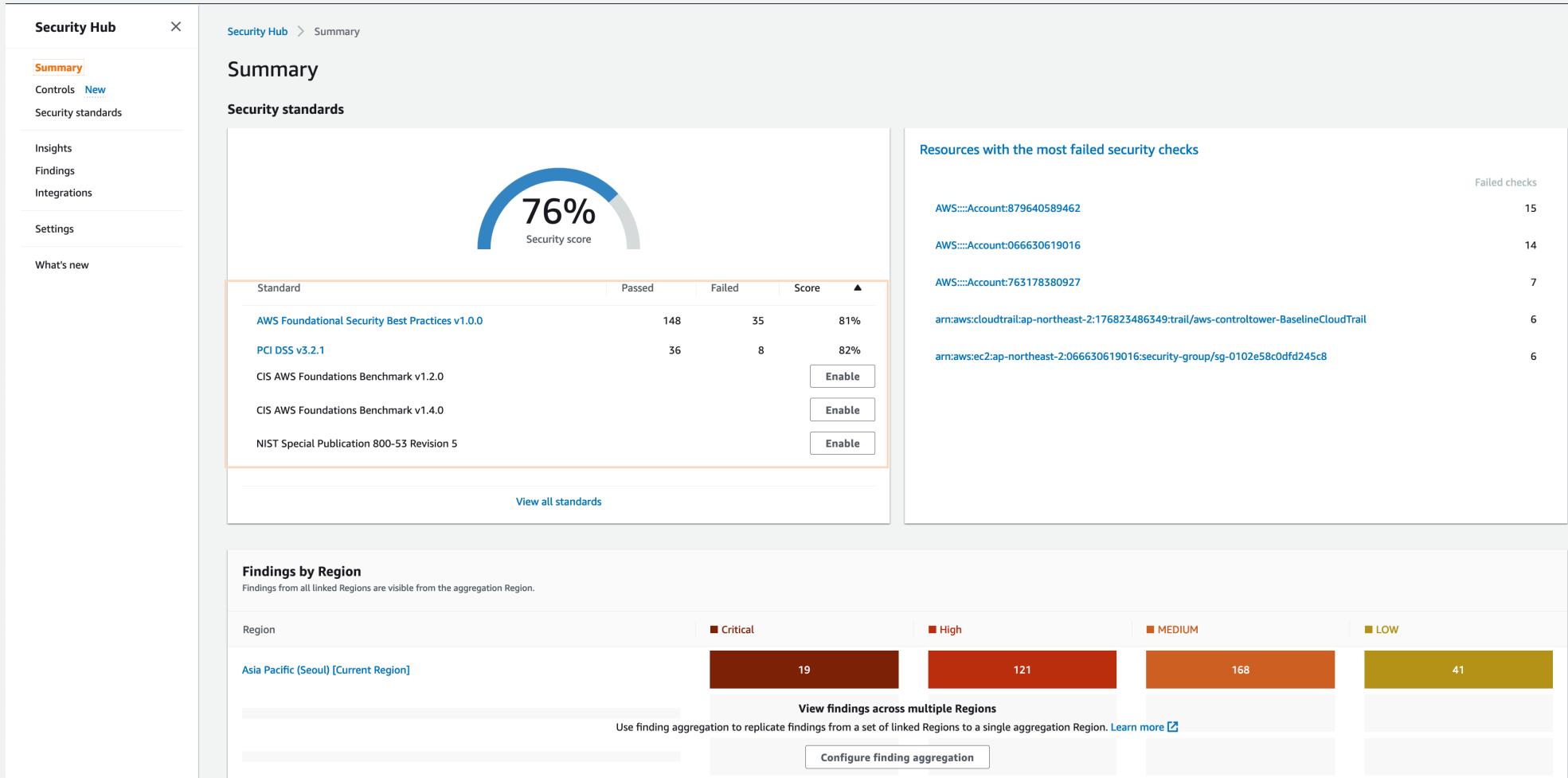
다중 계정 지원

- 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

Summary

Controls **New**

Security standards

Insights

Findings

Integrations

Settings

What's new

Security Hub > Findings

Findings (20+)

A finding is a security issue or a failed security check.

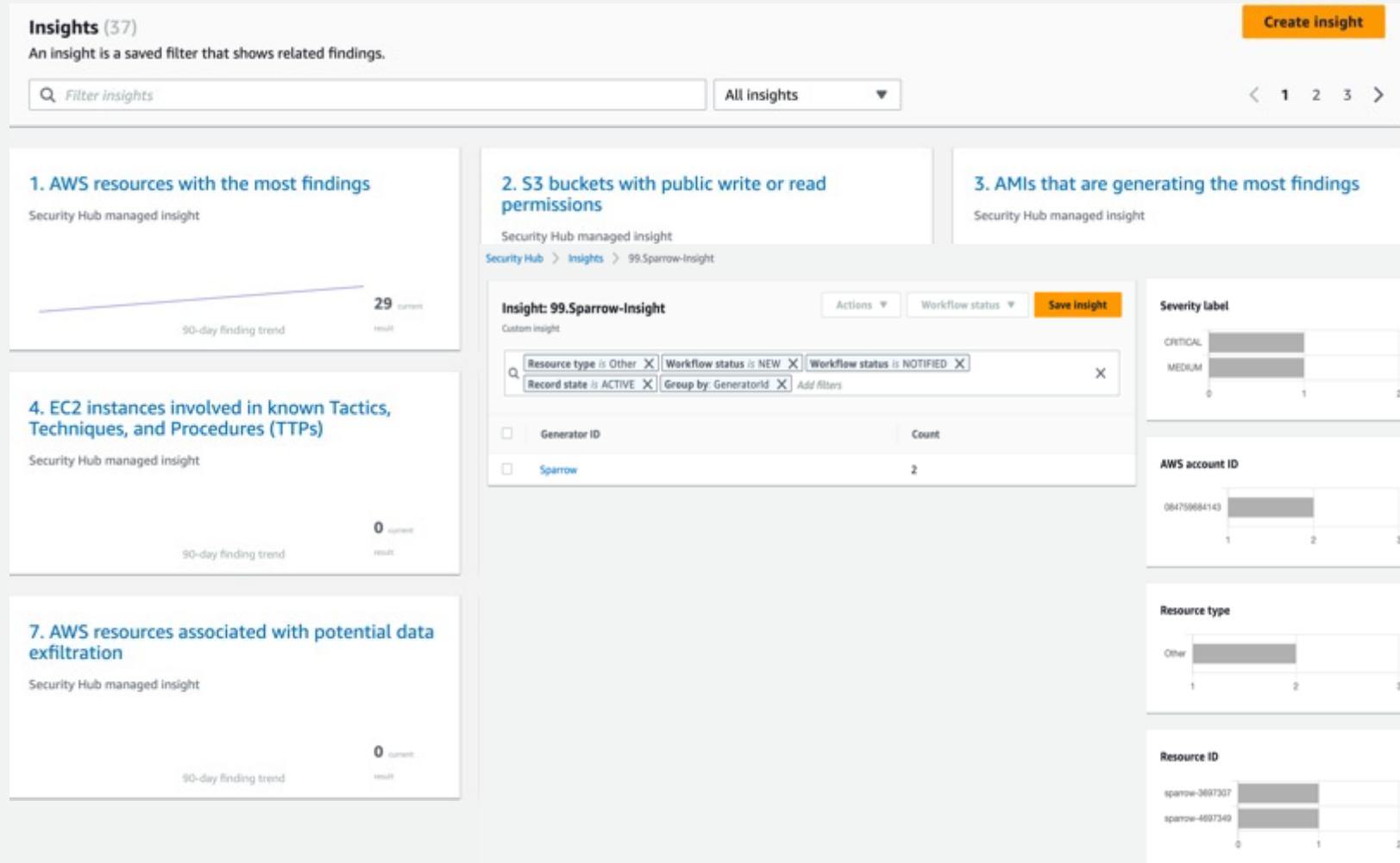
Add filters

Severity	Workflow status	Record State	Region	Account Id	Company	Product	Title	Resource	Compliance Status	Updated at
LOW	NEW	ACTIVE	ap-northeast-2	066630619016	AWS	Firewall Manager	Firewall Manager found redundant security group	EC2 Security Group sg-079c247f56de9a755	PASSED	a minute ago
LOW	NEW	ACTIVE	ap-northeast-2	066630619016	AWS	Firewall Manager	Firewall Manager found unused security group	EC2 Security Group sg-04c741d73c0ed25a7	PASSED	a minute ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	Config.1 AWS Config should be enabled	Account 879640589462	PASSED	6 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	2.8 Ensure rotation for customer created CMKs is enabled	Account 879640589462	PASSED	7 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	1.4 Ensure access keys are rotated every 90 days or less	Account 879640589462	PASSED	7 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	1.3 Ensure credentials unused for 90 days or greater are disabled	Account 879640589462	PASSED	7 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	1.22 Ensure IAM policies that allow full administrative privileges are not created	Account 879640589462	PASSED	7 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password	Account 879640589462	PASSED	7 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	1.16 Ensure IAM policies are attached only to groups or roles	Account 879640589462	PASSED	7 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	2.5 Ensure AWS Config is enabled	Account 879640589462	PASSED	10 minutes ago
INFORMATIONAL	RESOLVED	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	SSM.3 EC2 instances managed by Systems Manager should have an association compliance status of COMPLIANT	AwsSsmAssociationCompliance i-064c493987b15c1b6	PASSED	22 minutes ago
MEDIUM	NEW	ACTIVE	ap-northeast-2	879640589462	AWS	Security Hub	2.9 Ensure VPC flow logging is enabled in all VPCs	EC2 VPC vpc-0a153a562a8d00d23	FAILED	23 minutes ago



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)

The screenshot shows the AWS Security Hub Settings interface. At the top, there's a breadcrumb navigation: Security Hub > Settings. Below that, the title "Settings" is displayed above a horizontal navigation bar with five tabs: Accounts (highlighted in orange), Regions, Custom actions, Usage, and General. Under the "Accounts" tab, the heading "Accounts" is shown with an "Info" link and a refresh icon. At the bottom of this section, there are three buttons: "+ Add accounts" (white button), "Auto-enable accounts" (orange button with a blue icon), and "Auto-enable default standards" (gray button with a gray icon).

Security Hub 과금 기준

- Security Hub의 과금 기준은 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

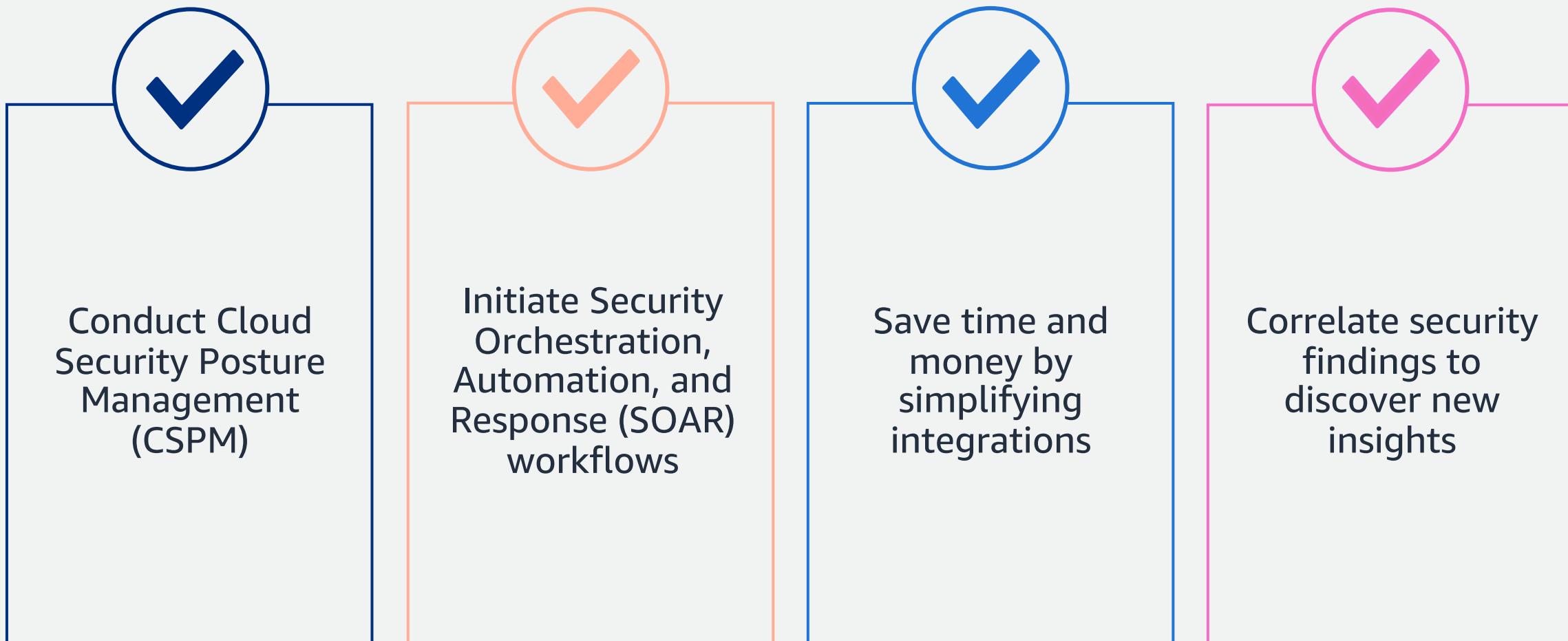
계정/리전/월당 최초 이벤트 10,000건 초과

이벤트당 0.00003 USD



Security Hub Use Case

Security Hub Use Case Overview



Posture Management – Use Case

Security Hub > Security standards > NIST Special Publication 800-53 Revision 5

NIST Special Publication 800-53 Revision 5

Overview

Security score: 73% (157 of 215 controls passed) | 240 of 710 checks failed | Chart legend: 34% failed

All enabled	Failed	Unknown	No data	Passed	Disabled
239	58	0	24	157	0

All enabled controls (239)

Compliance Status	Severity	ID	Title
Failed	Critical	EC2.19	Security groups should not allow unrestricted access to ports with high risk
Failed	Critical	IAM.6	Hardware MFA should be enabled for the root user
Failed	Critical	IAM.9	Virtual MFA should be enabled for the root user
Failed	High	CodeBuild.5	CodeBuild project environments should not have privileged mode enabled
Failed	High	EC2.8	EC2 instances should use Instance Metadata Service Version 2 (IMDSv2)
Failed	High	S3.8	S3 Block Public Access setting should be enabled at the bucket-level
Failed	High	EC2.2	The VPC default security group should not allow inbound and outbound traffic
Failed	High	EC2.9	EC2 instances should not have a public IPv4 address
Failed	High	EC2.13	Security groups should not allow ingress from 0.0.0.0/0 to port 22

Security standards

AWS Foundational Security Best Practices v1.0.0 by AWS Security Hub

Description: The AWS Foundational Security Best Practices standard is a set of automated security checks that detect when AWS accounts and deployed resources do not align with security best practices. The standard is defined by AWS security experts. This curated set of controls helps improve your security posture in AWS, and covers AWS's most popular and foundational services.

Security score: 77% (Updated 9 hours ago)

CIS AWS Foundations Benchmark v1.2.0 by AWS Security Hub

Description: The Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score: 35% (Updated 9 hours ago)

CIS AWS Foundations Benchmark v1.4.0 by AWS Security Hub

Description: The Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 is a set of security configuration best practices for AWS. This Security Hub standard automatically checks for your compliance readiness against a subset of CIS requirements.

Security score: 73% (Updated 9 hours ago)

PCI DSS v3.2.1 by AWS Security Hub

Description: The Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 is an information security standard for entities that store, process, and/or transmit cardholder data. This Security Hub standard automatically checks for your compliance readiness against a subset of PCI DSS requirements.

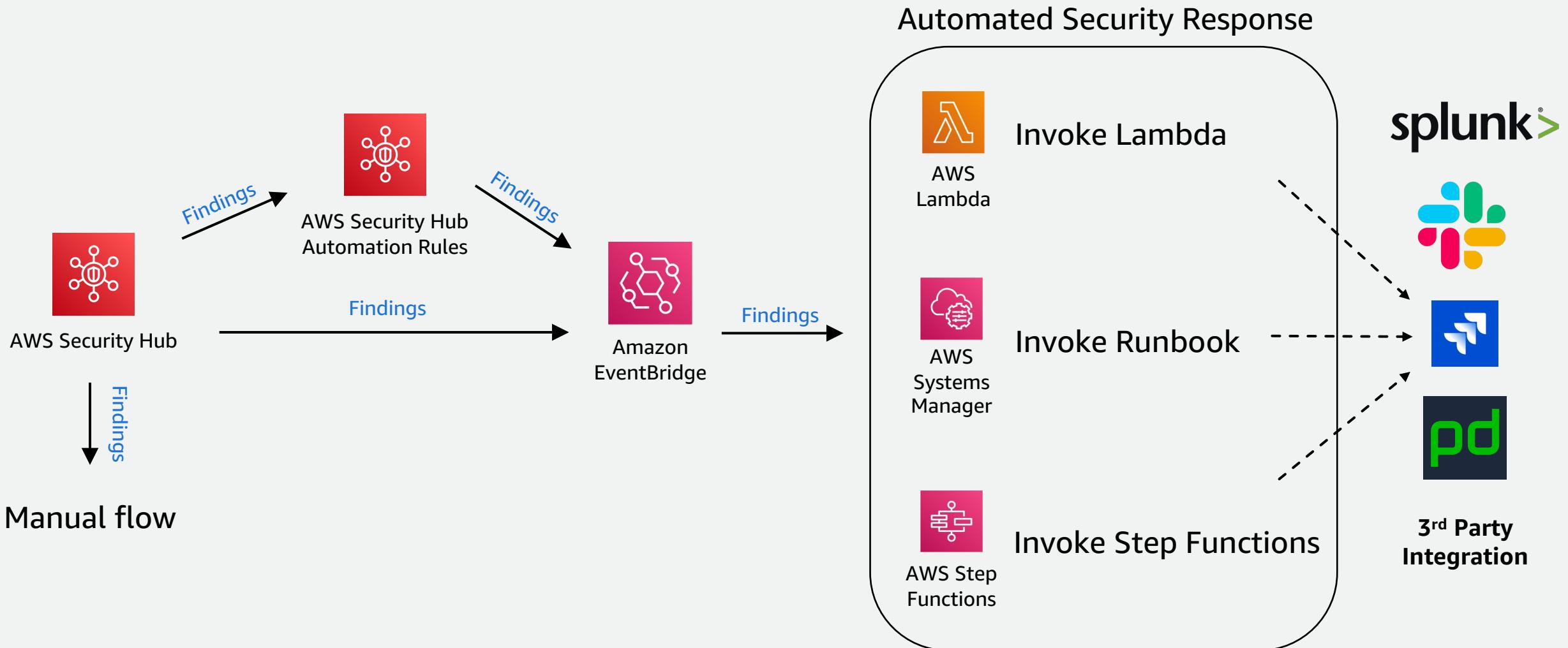
Security score: 100% (Updated 9 hours ago)

Service-Managed Standard: AWS Control Tower by AWS Control Tower

Description: The standard is created and managed by AWS Control Tower. Any Security Hub controls managed by AWS Control Tower will be reflected in this standard. The standard can only be disabled and deleted via AWS Control Tower. [Learn More](#)



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.

Security Hub > Automations > Create rule

Create rule

Rule Type

Create a rule from template
use a pre-populated template for common scenario

Create custom rule
Start with all blank

Rule template

Elevate severity for important resources

Elevate severity for important resources

Suppress informational findings

Elevate severity for production accounts

Rule name

Elevate severity for important resources

The name must have 3 to 28 characters. Valid characters are a-z (lowercase only), 0-9, and - (hyphen)

Rule description

Elevate finding severity to Critical when specific S3 bucket at risk

Criteria

Choose which findings your rule applies to

Security Hub > Automations > Elevate severity for findings related to Crown Jewels resources

Elevate severity for findings related to Crown Jewels resources

Edit

Rule

Rule name: Elevate severity for findings related to Crown Jewels resources

Rule description: Setting finding's severity to Critical for specific finding's resource ID

Criteria

Key	Operator	Value
ResourceId	EQUALS	arn:aws:s3:::examplebucket/developers/design_info.doc
WorkflowStatus	EQUALS	NEW

Automated action

Severity	Note
CRITICAL	Need urgent look into this critical S3 bucket

Use cases

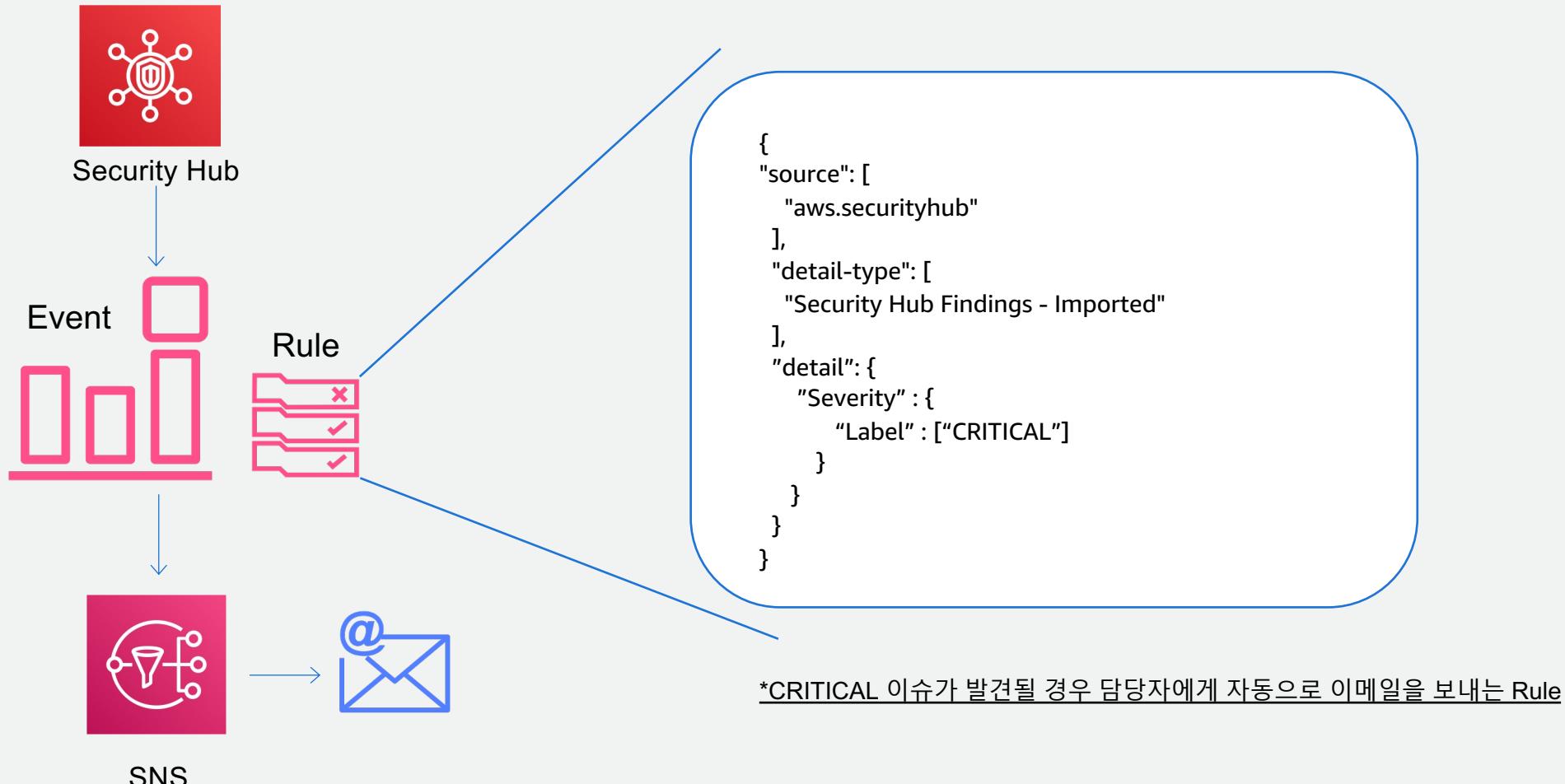
- Changing finding severity
- Suppressing findings
- Adding notes

aws

19

Security Hub Use Case - Automation and Response

- 다른 AWS 서비스와 연계한 자동화 작업 가능



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 security findings – Use case

Security Hub > Insights > 9. S3 buckets that don't meet security standards / best practice

Insight: 9. S3 buckets that don't meet security standards / best practice

Security Hub managed insight

Add filter

Type is Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices × Type is Software and Configuration Checks/Industry and Regulatory Standards ×

Resource type is AwsS3Bucket × Resource type is AWS::S3::Bucket × Workflow status is NEW × Workflow status is NOTIFIED × Record state is ACTIVE × Group by: ResourceId ×

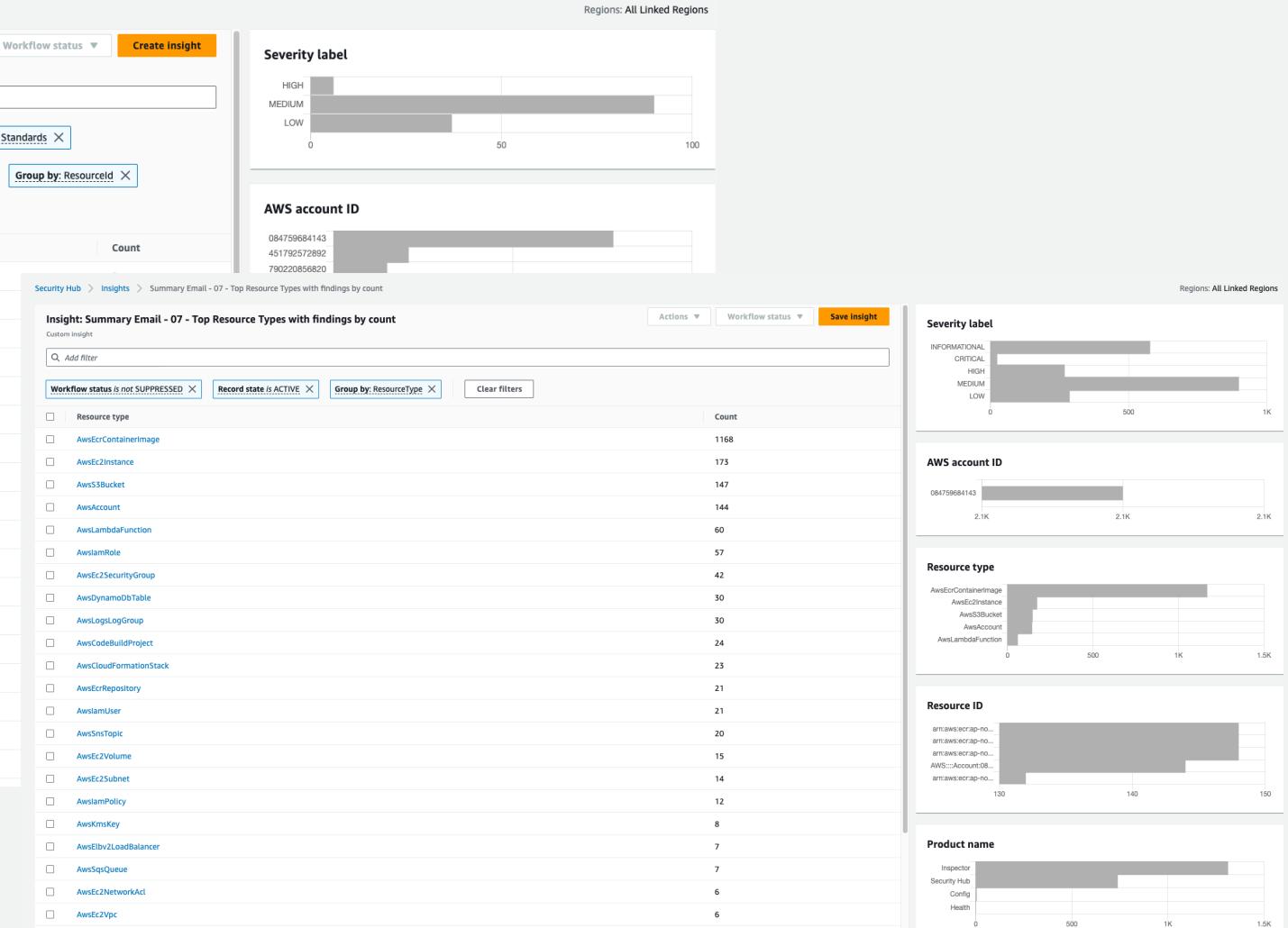
Clear filters

Count
Resource ID
arn:aws:s3::sc-terraform-engine-logging-084759684143-ap-northeast-2
arn:aws:s3::tf-state-workshop-a27d7f045cdb58db
arn:aws:s3::cf-templates-1jo1kvrh2ypoo-ap-northeast-2
arn:aws:s3::inspector-export-bucket-an2-kt
arn:aws:s3::kdaegon-flow-log-bucket-084759684143
arn:aws:s3::kdaegon-tf-backend
arn:aws:s3::pks-dev-bucket-084759684143
arn:aws:s3::terraform-engine-bootstrap-084759684143-ap-northeast-2
arn:aws:s3::kdaegon-sparrow-test-sample
arn:aws:s3::sc-terraform-engine-state-084759684143-ap-northeast-2
arn:aws:s3::cf-stack-customcontroltowers3accesslogsbucket-624b0pf11zv8
arn:aws:s3::kdaegon-demo-bucket-01010101
arn:aws:s3::pks-prod-bucket-790220856820
arn:aws:s3::sc-790220856820-pp-k5eadwfdsxncs-s3bucket-1iwymzf9znxr
arn:aws:s3::cf-templates-pmwkttm1s8yo-ap-northeast-2
arn:aws:s3::cfct-stack-customcontroltowercloudtraildataeventb-bpkpmga8j3hu
arn:aws:s3::cfct-stack-customcontroltowerpipelineartifacts3bu-1d44vjqgk0f9l
arn:aws:s3::custom-control-tower-configuration-451792572892-ap-northeast-2

Security Hub Custom Insight



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Demo



Thank you!