



AWSKRUG

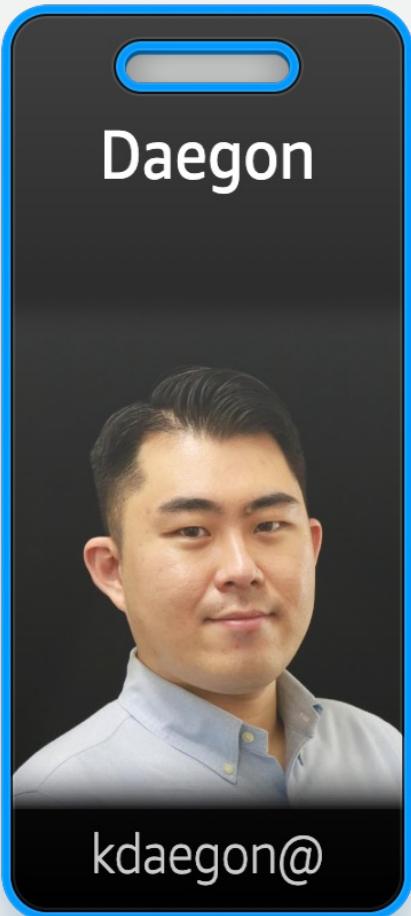
# Security Hub

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.

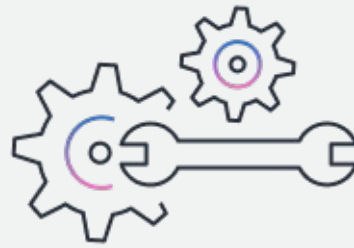
# Agenda

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

# Security and compliance challenges



**Lack of visibility into  
security risks**

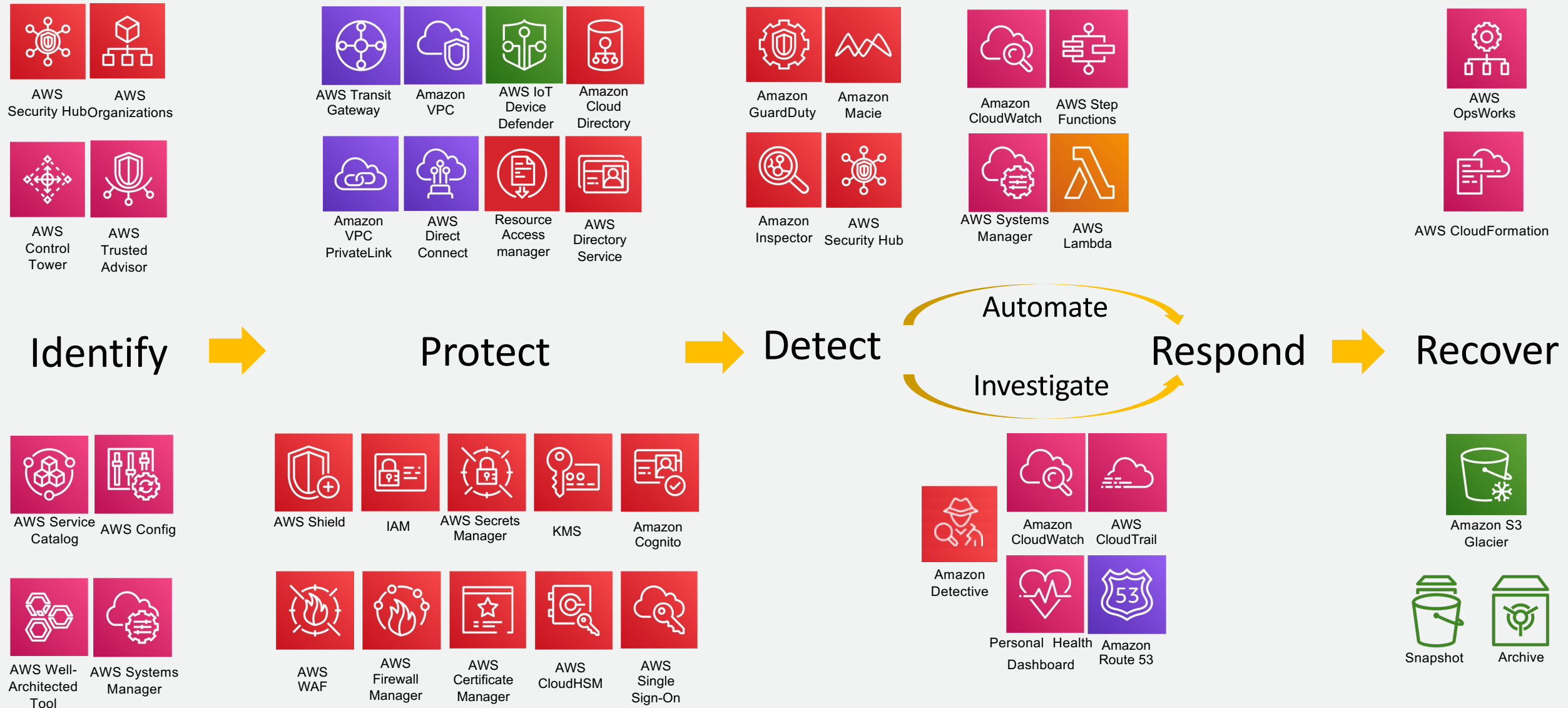


**Complexity of tools,  
vendors, and processes**



**Too many alerts, and not  
enough security experts**

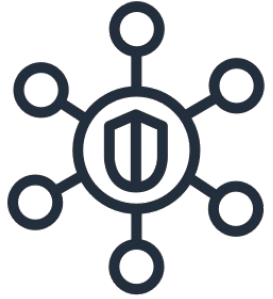
# AWS Foundational and Layered Security Services



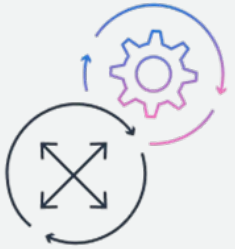
# Security Hub Overview



# What is AWS Security Hub?



AWS Security Hub는 보안 모범 사례 점검을 지속적으로 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

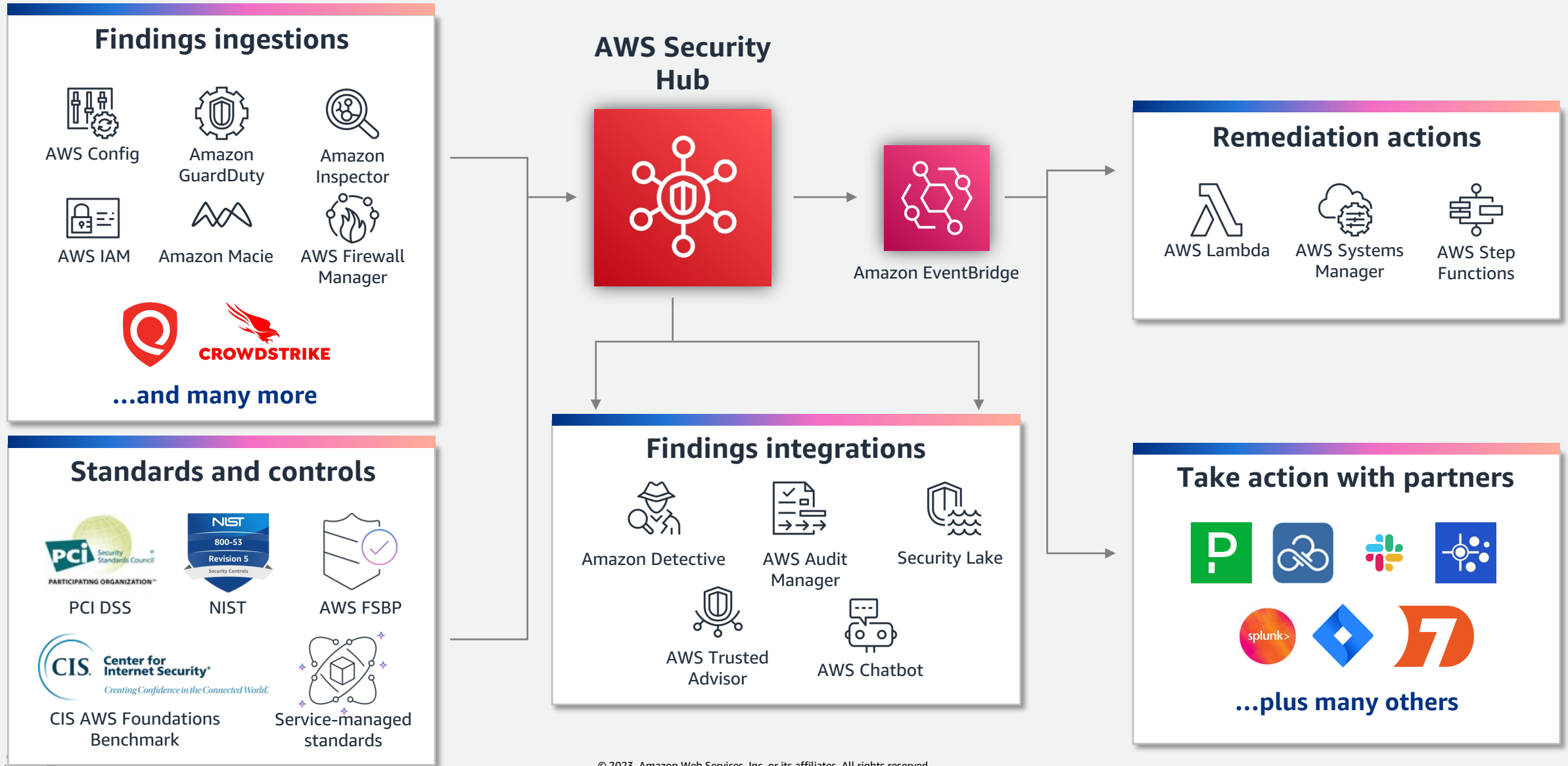


규제 및 특정  
프레임워크에  
부합하는 보안  
표준 제공



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

# 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

Summary

Controls

Security standards

Insights

Findings

Integrations

Settings

What's new

Security Hub > Summary

Summary

Security standards

76%

Security score

| Standard  | Passed | Failed | Score             |
|---|--------|--------|-------------------|
| <a href="#">AWS Foundational Security Best Practices v1.0.0</a> | 148    | 35     | 81%               |
| <a href="#">PCI DSS v3.2.1</a>                                  | 36     | 8      | 82%               |
| CIS AWS Foundations Benchmark v1.2.0                            |        |        | <div>Enable</div> |
| CIS AWS Foundations Benchmark v1.4.0                            |        |        | <div>Enable</div> |
| NIST Special Publication 800-53 Revision 5                      |        |        | <div>Enable</div> |

View all standards

Resources with the most failed security checks

|  | Failed checks |
|--|---------------|
| <a href="#">AWS:::Account:879640589462</a>   | 15            |
| <a href="#">AWS:::Account:066630619016</a>   | 14            |
| <a href="#">AWS:::Account:763178380927</a>   | 7             |
| <a href="#">arn:aws:cloudtrail:ap-northeast-2:176823486349:trail/aws-controltower-BaselineCloudTrail</a> | 6             |
| <a href="#">arn:aws:ec2:ap-northeast-2:066630619016:security-group/sg-0102e58c0dfd245c8</a>              | 6             |

Findings by Region

Findings from all linked Regions are visible from the aggregation Region.

| Region  | Critical | High | MEDIUM | LOW |
|---|----------|------|--------|-----|
| <a href="#">Asia Pacific (Seoul) [Current Region]</a> | 19       | 121  | 168    | 41  |

View findings across multiple Regions

Use finding aggregation to replicate findings from a set of linked Regions to a single aggregation Region. [Learn more](#)

Configure finding aggregation



# 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.

Q Add filters

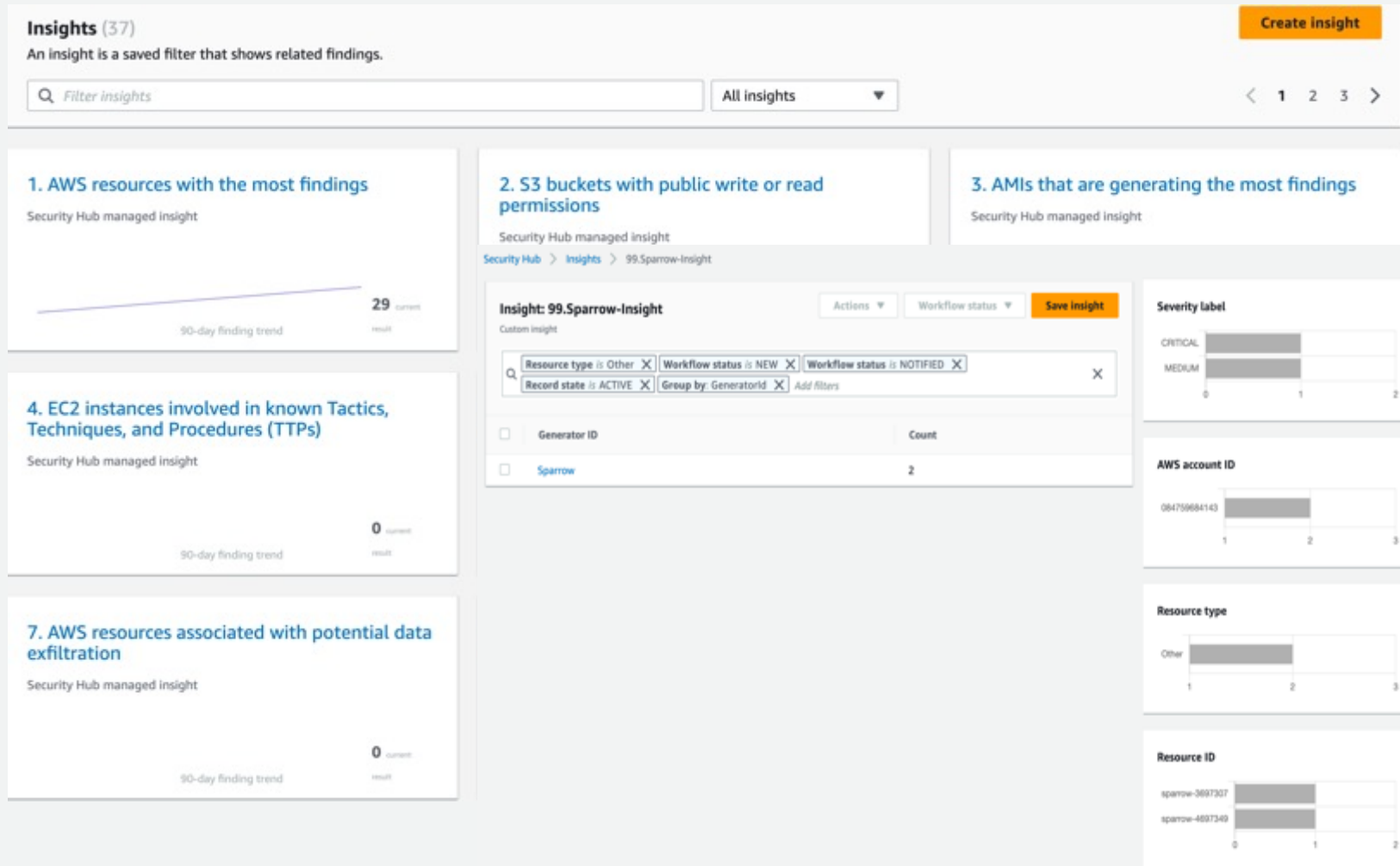
< 1 ... >

| <input type="checkbox"/> | Severity      | Workflow status | Record State | Region         | Account Id   | Company | Product          | Title  | Resource   | Compliance Status | Updated at     |
|--------------------------|---------------|-----------------|--------------|----------------|--------------|---------|------------------|--|--|-------------------|----------------|
| <input type="checkbox"/> | LOW           | NEW             | ACTIVE       | ap-northeast-2 | 066630619016 | AWS     | Firewall Manager | Firewall Manager found redundant security group  | EC2 Security Group<br>sg-079c247f56de9a755         |                   | a minute ago   |
| <input type="checkbox"/> | LOW           | NEW             | ACTIVE       | ap-northeast-2 | 066630619016 | AWS     | Firewall Manager | Firewall Manager found unused security group   | EC2 Security Group<br>sg-04c741d73c0ed25a7         |                   | a minute ago   |
| <input type="checkbox"/> | INFORMATIONAL | RESOLVED        | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | Config.1 AWS Config should be enabled  | Account<br>879640589462                            | PASSED            | 6 minutes ago  |
| <input type="checkbox"/> | INFORMATIONAL | RESOLVED        | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | 2.8 Ensure rotation for customer created CMKs is enabled   | Account<br>879640589462                            | PASSED            | 7 minutes ago  |
| <input type="checkbox"/> | INFORMATIONAL | RESOLVED        | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | 1.4 Ensure access keys are rotated every 90 days or less   | Account<br>879640589462                            | PASSED            | 7 minutes ago  |
| <input type="checkbox"/> | INFORMATIONAL | RESOLVED        | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | 1.3 Ensure credentials unused for 90 days or greater are disabled  | Account<br>879640589462                            | PASSED            | 7 minutes ago  |
| <input type="checkbox"/> | INFORMATIONAL | RESOLVED        | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | 1.22 Ensure IAM policies that allow full "*,*" administrative privileges are not created                 | Account<br>879640589462                            | PASSED            | 7 minutes ago  |
| <input type="checkbox"/> | 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<br>879640589462                            | PASSED            | 7 minutes ago  |
| <input type="checkbox"/> | INFORMATIONAL | RESOLVED        | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | 1.16 Ensure IAM policies are attached only to groups or roles  | Account<br>879640589462                            | PASSED            | 7 minutes ago  |
| <input type="checkbox"/> | INFORMATIONAL | RESOLVED        | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | 2.5 Ensure AWS Config is enabled   | Account<br>879640589462                            | PASSED            | 10 minutes ago |
| <input type="checkbox"/> | 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<br>i-064c493987b15c1b6 | PASSED            | 22 minutes ago |
| <input type="checkbox"/> | MEDIUM        | NEW             | ACTIVE       | ap-northeast-2 | 879640589462 | AWS     | Security Hub     | 2.9 Ensure VPC flow logging is enabled in all VPCs   | EC2 VPC<br>vpc-0a153a562a8d00d23                   | FAILED            | 23 minutes ago |



# Security Hub Insights

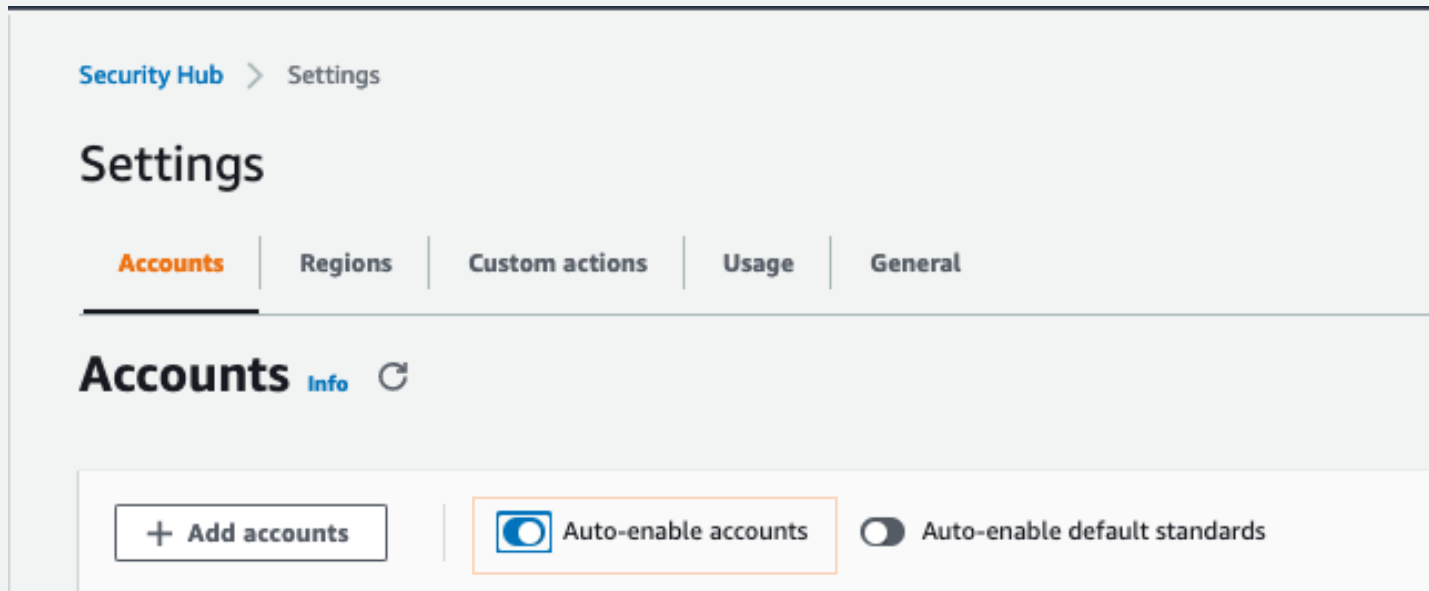
- 주의가 필요한 리소스 및 취약점에 대해 인사이트를 생성하여 관리 가능



- 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)



# 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



Conduct Cloud  
Security Posture  
Management  
(CSPM)



Initiate Security  
Orchestration,  
Automation, and  
Response (SOAR)  
workflows



Save time and  
money by  
simplifying  
integrations



Correlate security  
findings to  
discover new  
insights



# 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

34% failed

Chart legend

All enabled

239

Failed

58

Unknown

0

No data

24

Passed

157

Disabled

0

All enabled controls (239)

Filter all enabled controls

| 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

Disable

View results

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

Disable

View results

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.

Enable

NIST Special Publication 800-53 Revision 5

by AWS Security Hub

Description

NIST Special Publication 800-53 Revision 5 provides a catalog of security and privacy controls for information systems and organizations. This Security Hub standard automatically checks for your compliance readiness against a subset of NIST 800-53 RS requirements.

Security score

73%

Updated 9 hours ago

Disable

View results

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.

Enable

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 score

100%

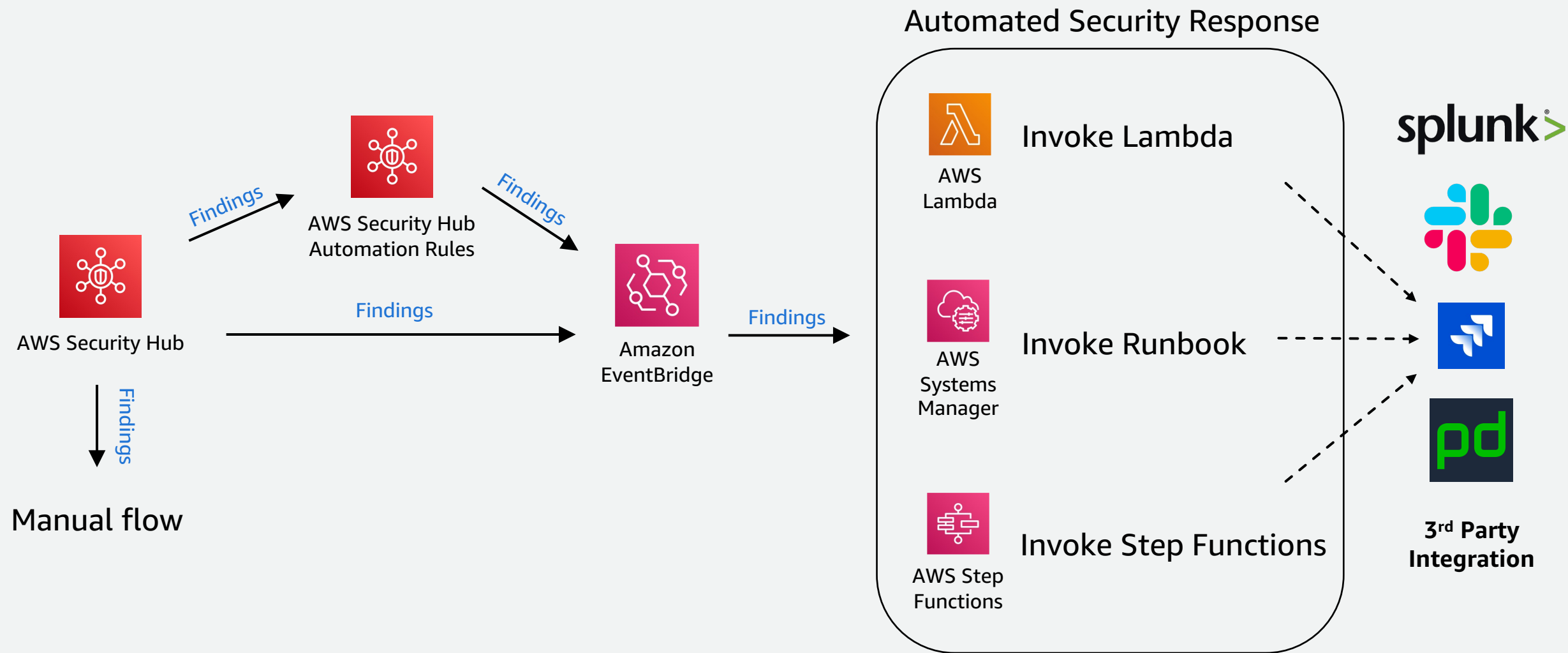
Updated 9 hours ago

Disable

View results



# 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 fields

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

## Use cases

- Changing finding severity
- Suppressing findings
- Adding notes

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

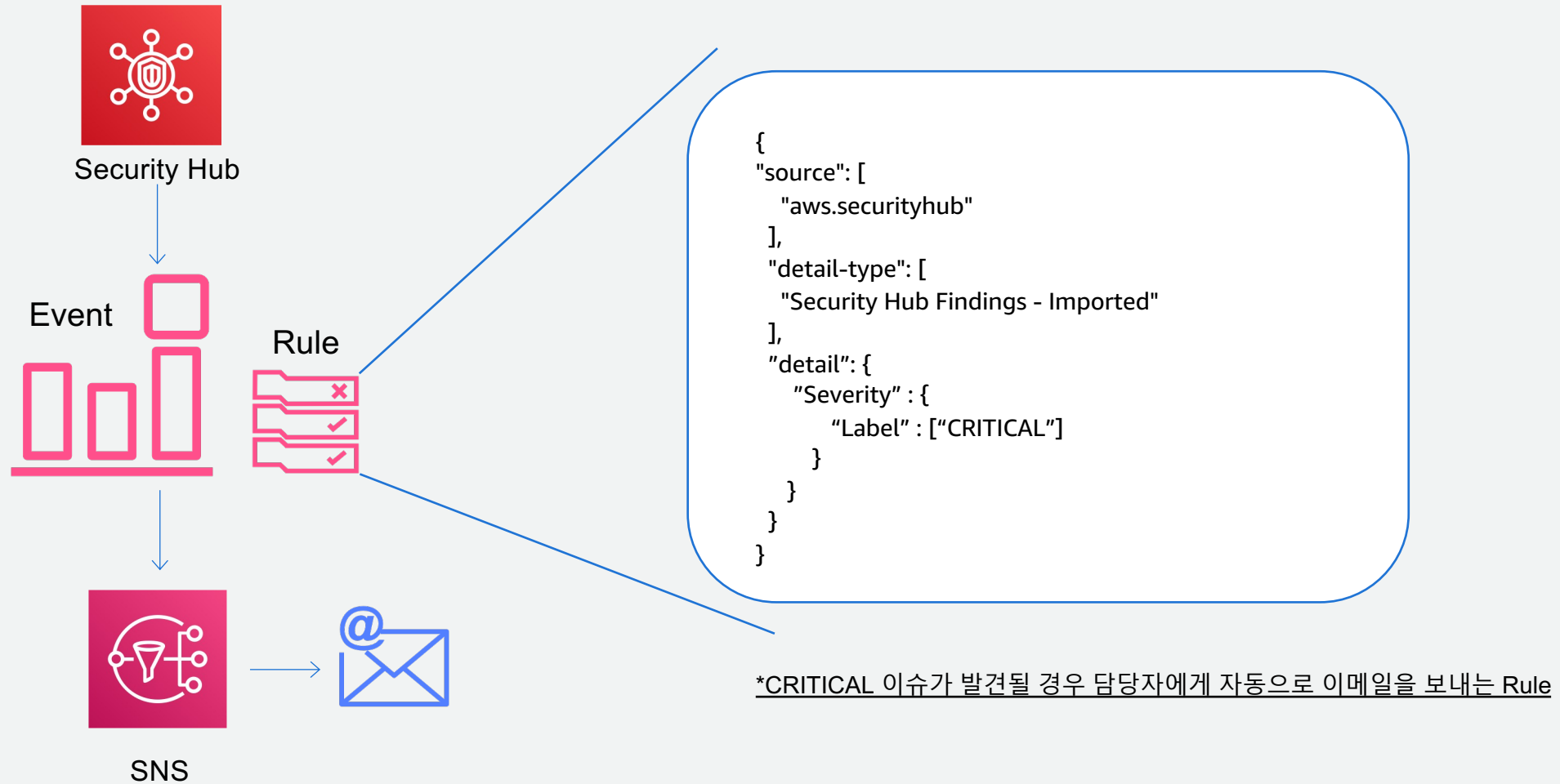
|                |          |   |
|----------------|----------|---|
| Key            | Operator | Value   |
| ResourceId     | EQUALS   | arn:aws:s3:::examplebucket/developers/design_info.doc |
| WorkflowStatus | EQUALS   | NEW   |

Automated action

|          |   |
|----------|---|
| Severity | Note  |
| CRITICAL | Need urgent look into this critical S3 bucket |

# 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                     |
|--|-------------------------------|
| <a href="#">AWS Config</a>   | Sends findings                |
| <a href="#">AWS Firewall Manager</a>                               | Sends findings                |
| <a href="#">Amazon GuardDuty</a>                                   | Sends findings                |
| <a href="#">AWS Health</a>   | Sends findings                |
| <a href="#">AWS Identity and Access Management Access Analyzer</a> | Sends findings                |
| <a href="#">Amazon Inspector</a>                                   | Sends findings                |
| <a href="#">AWS IoT Device Defender</a>                            | Sends findings                |
| <a href="#">Amazon Macie</a>                                       | Sends findings                |
| <a href="#">AWS Systems Manager Patch Manager</a>                  | Sends findings                |
| <a href="#">AWS Audit Manager</a>                                  | Receives findings             |
| <a href="#">AWS Chatbot</a>  | Receives findings             |
| <a href="#">Amazon Detective</a>                                   | Receives findings             |
| <a href="#">Amazon Security Lake</a>                               | Receives findings             |
| <a href="#">AWS Systems Manager Explorer and OpsCenter</a>         | Receives and updates findings |
| <a href="#">AWS Trusted Advisor</a>                                | Receives findings             |

## AWS Native Integration

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

## 3rd Party Product Integration



# Correlate securiry 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

Q Add filter

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

Type is Software and Configuration Checks/Industry and Regulatory Standards X

Resource type is AwsS3Bucket X

Resource type is AWS::S3::Bucket X

Workflow status is NEW X

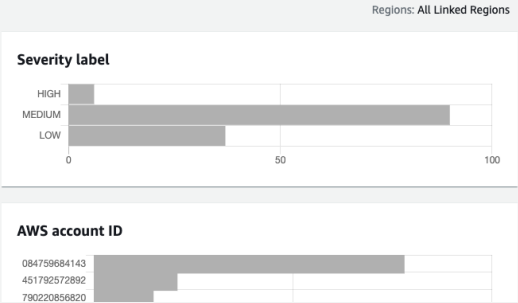
Workflow status is NOTIFIED X

Record state is ACTIVE X

Group by: ResourceId X

Clear filters

| Resource ID   | Count |
|---|-------|
| 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::cfct-stack-customcontroltowers3accesslogsbucket-624b0pf11zv8    |       |
| arn:aws:s3::kdaegon-demo-bucket-01010101                                    |       |
| arn:aws:s3::pks-prod-bucket-790220856820                                    |       |
| arn:aws:s3::sc-790220856820-pp-k5eadwfdxnscs-s3bucket-1lwymzf9znzxr         |       |
| arn:aws:s3::cf-templates-pmwkttmis8yo-ap-northeast-2                        |       |
| arn:aws:s3::cfct-stack-customcontroltowercloudtraildataeventb-bpkpma8j3hu   |       |
| arn:aws:s3::cfct-stack-customcontroltowerpipelineartifacts3bu-1d44vjgqk0f9l |       |
| arn:aws:s3::custom-control-tower-configuration-451792572892-ap-northeast-2  |       |



Security Hub > Insights > Summary Email - 07 - Top Resource Types with findings by count

Insight: Summary Email - 07 - Top Resource Types with findings by count

Custom insight

Q Add filter

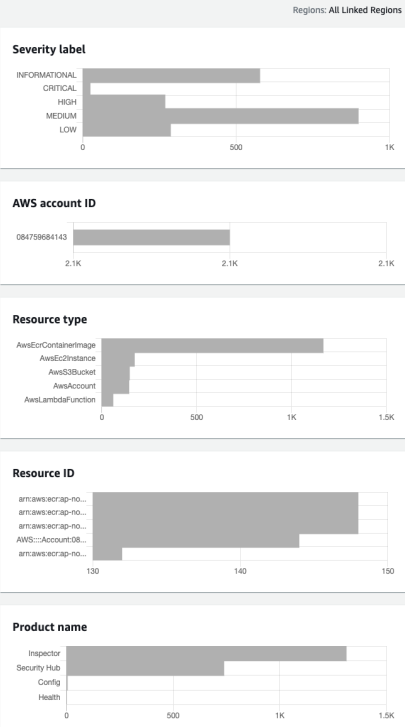
Workflow status is not SUPPRESSED X

Record state is ACTIVE X

Group by: ResourceType X

Clear filters

| Resource type          | Count |
|------------------------|-------|
| AwsEcrContainerImage   | 1168  |
| AwsEc2Instance         | 173   |
| AwsS3Bucket            | 147   |
| AwsAccount             | 144   |
| AwsLambdaFunction      | 60    |
| AwsIamRole             | 57    |
| AwsEc2SecurityGroup    | 42    |
| AwsDynamoDbTable       | 30    |
| AwsLogsLogGroup        | 30    |
| AwsCodeBuildProject    | 24    |
| AwsCloudFormationStack | 23    |
| AwsEcrRepository       | 21    |
| AwsIamUser             | 21    |
| AwsSnsTopic            | 20    |
| AwsEc2Volume           | 15    |
| AwsEc2Subnet           | 14    |
| AwsIamPolicy           | 12    |
| AwsKmsKey              | 8     |
| AwsElbv2LoadBalancer   | 7     |
| AwsSqsQueue            | 7     |
| AwsEc2NetworkAcl       | 6     |
| AwsEc2Vpc              | 6     |



Securiry Hub Custom Insight



# Demo





# Thank you!