AWS Security Hub

Automated compliance checks and security alert prioritization

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Table of contents

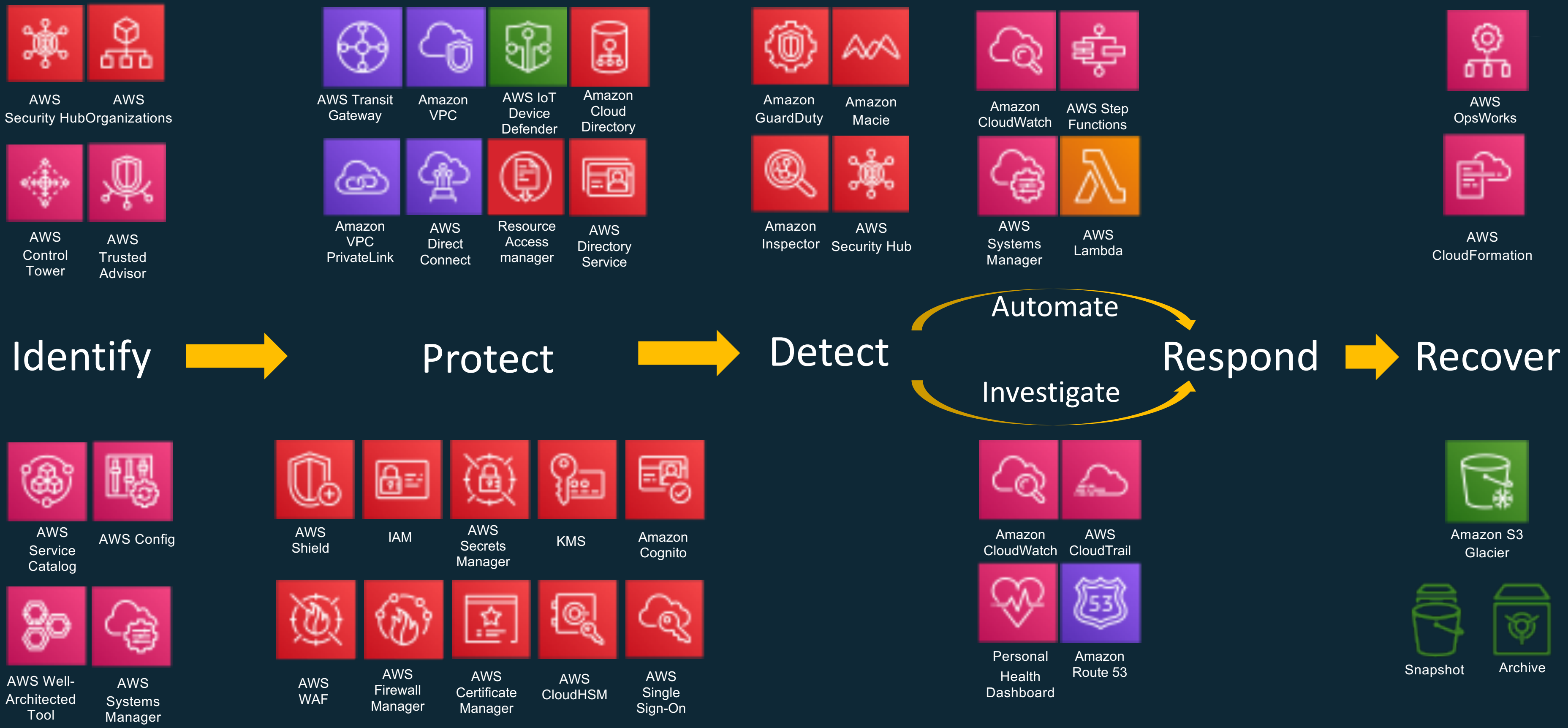
- AWS Security Services overview
- Introduction AWS Security Hub
- AWS Security Hub Benefits
- Service Availability
- Pricing
- Customer References & Use Case
- Getting Started
- Partner Integrations
- Additional Resources

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Security Services overview

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Foundational and Layered Security Services



AWS Security Hub

AWS Organizations

AWS Control Tower

AWS Trusted Advisor

Identify

AWS Service Catalog

AWS Config

AWS Well-Architected Tool

AWS Systems Manager

AWS Transit Gateway

Amazon VPC

AWS IoT Device Defender

Amazon Cloud Directory

Amazon VPC PrivateLink

AWS Direct Connect

Resource Access manager

AWS Directory Service

Protect

AWS Shield

IAM

AWS Secrets Manager

KMS

Amazon Cognito

AWS WAF

AWS Firewall Manager

AWS Certificate Manager

AWS CloudHSM

AWS Single Sign-On

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

Detect

Automate

Investigate

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Respond

Amazon CloudWatch

AWS CloudTrail

Personal Health Dashboard

Amazon Route 53

AWS OpsWorks

AWS CloudFormation

Recover

Amazon S3 Glacier

Snapshot

Archive

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Introduction AWS Security Hub

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Problem statements

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

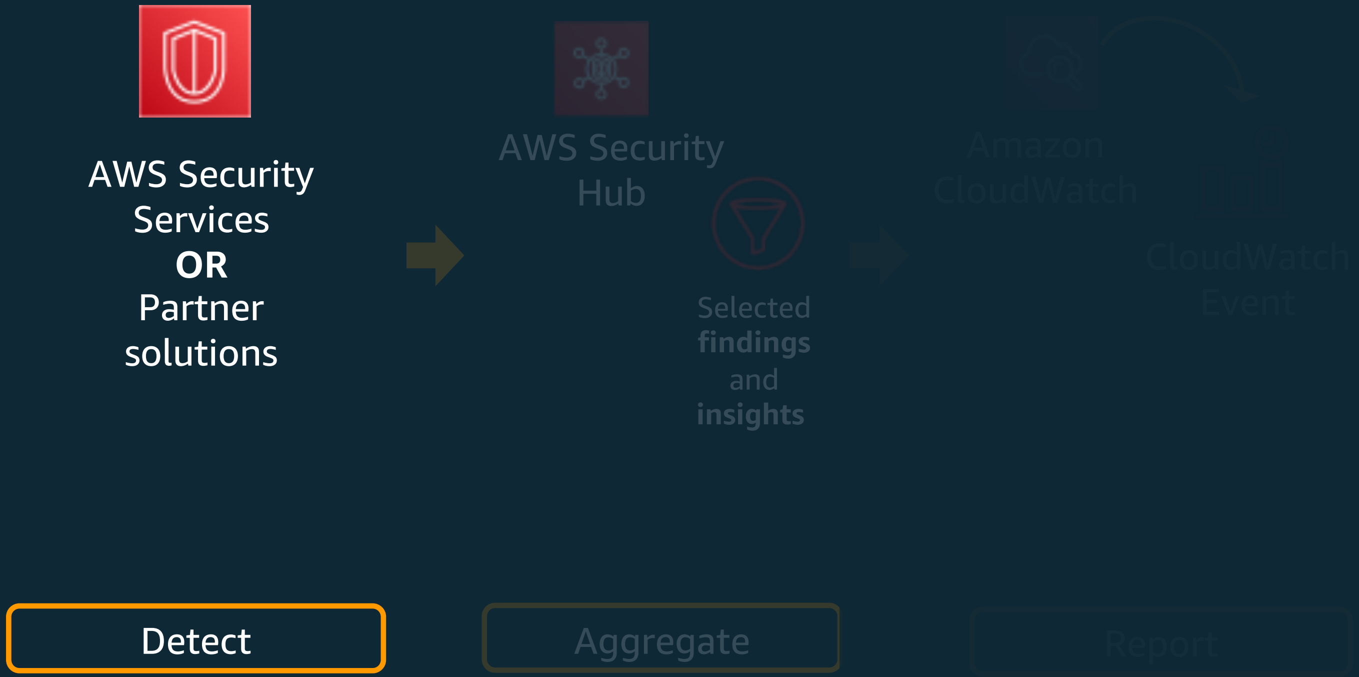
Introduction to AWS Security Hub

Better visibility into **security issues**. Easier to stay in **compliance**.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Introduction to AWS Security Hub

Responding to Findings \ Insights: *Remediation*



AWS Security Services **OR** Partner solutions

AWS Security Hub

Selected **findings** and **insights**

Amazon CloudWatch

CloudWatch Event

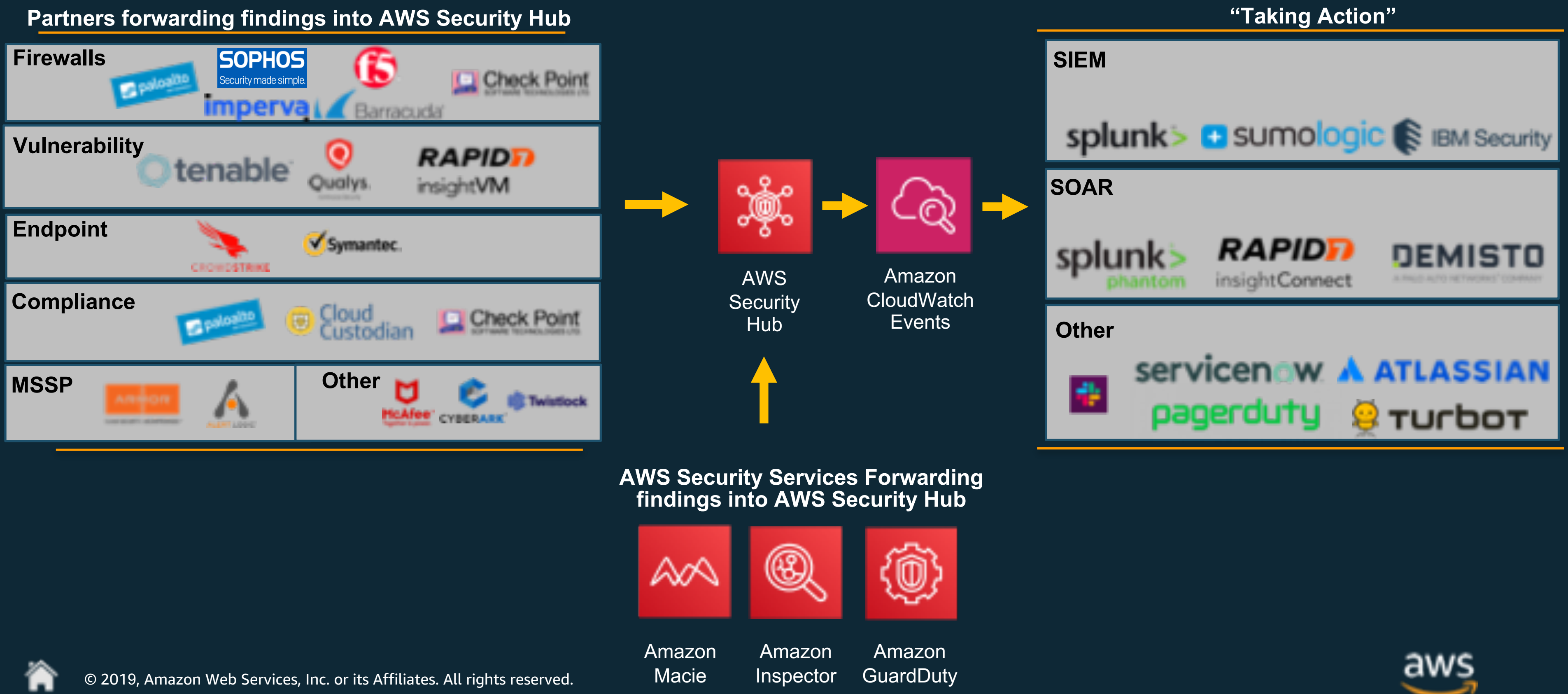
Detect

Aggregate

Report

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Partner integrations



Partners forwarding findings into AWS Security Hub

Firewalls

Vulnerability

Endpoint

Compliance

MSSP

Other

AWS Security Hub

Amazon CloudWatch Events

AWS Security Services Forwarding findings into AWS Security Hub

Amazon Macie

Amazon Inspector

Amazon GuardDuty

"Taking Action"

SIEM

SOAR

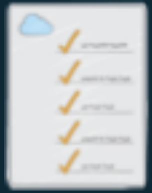
Other

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Security Hub Benefits

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Security Hub Benefits



Compliance standards

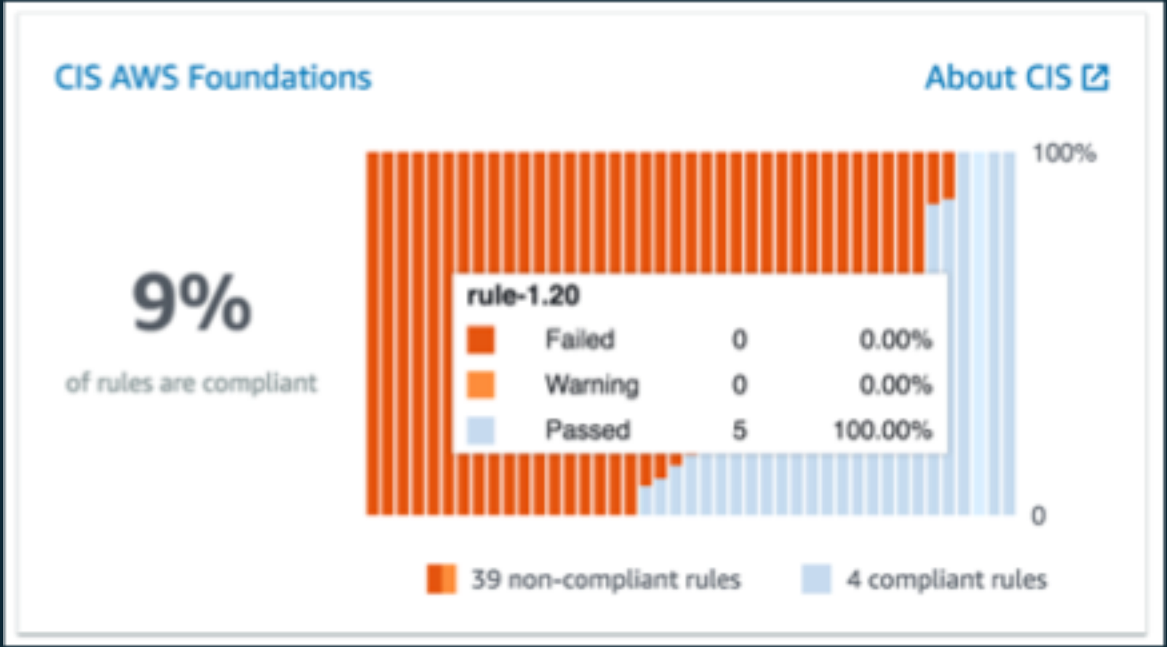
Aggregated findings

Take Action

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Automated compliance checks

CIS. Center for Internet Security®



CIS AWS Foundations

About CIS

9%

of rules are compliant

rule-1.20

🟥	Failed	0	0.00%
🟧	Warning	0	0.00%
🟦	Passed	5	100.00%

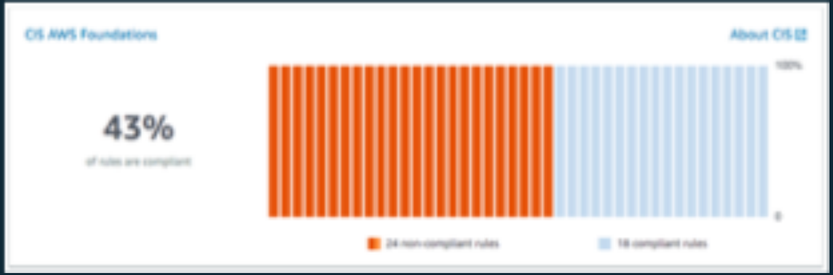
🟥 39 non-compliant rules

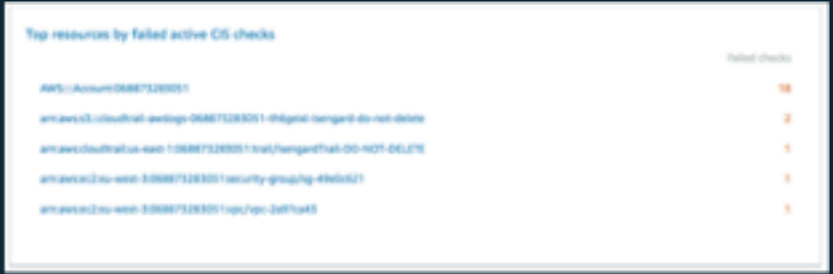
🟦 4 compliant rules

43 fully automated, nearly continuous checks

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Compliance Standards





Top resources by failed active CIS checks

	Failed checks
AWS::Account:068873283051	18
arn:aws:s3:::cloudtrail-awslogs-068873283051-th6geiei-isengard-do-not-delete	2
arn:aws:cloudtrail:us-east-1:068873283051:trail/IsengardTrail-DO-NOT-DELETE	1
arn:aws:ec2:eu-west-3:068873283051:security-group/sg-49e0c621	1
arn:aws:ec2:eu-west-3:068873283051:vpc/vpc-2a97ca43	1

CIS. Center for Internet Security®

Based on CIS AWS Foundations Benchmark

- 43 fully automated, nearly continuous checks
- Findings are displayed on main dashboard for quick access.
- Best practices information is provided to help mitigate gaps to be in compliance.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Compliance Standards

Examples:

Avoid the use of the **"root" account**

Ensure **CloudTrail** is enabled in all regions

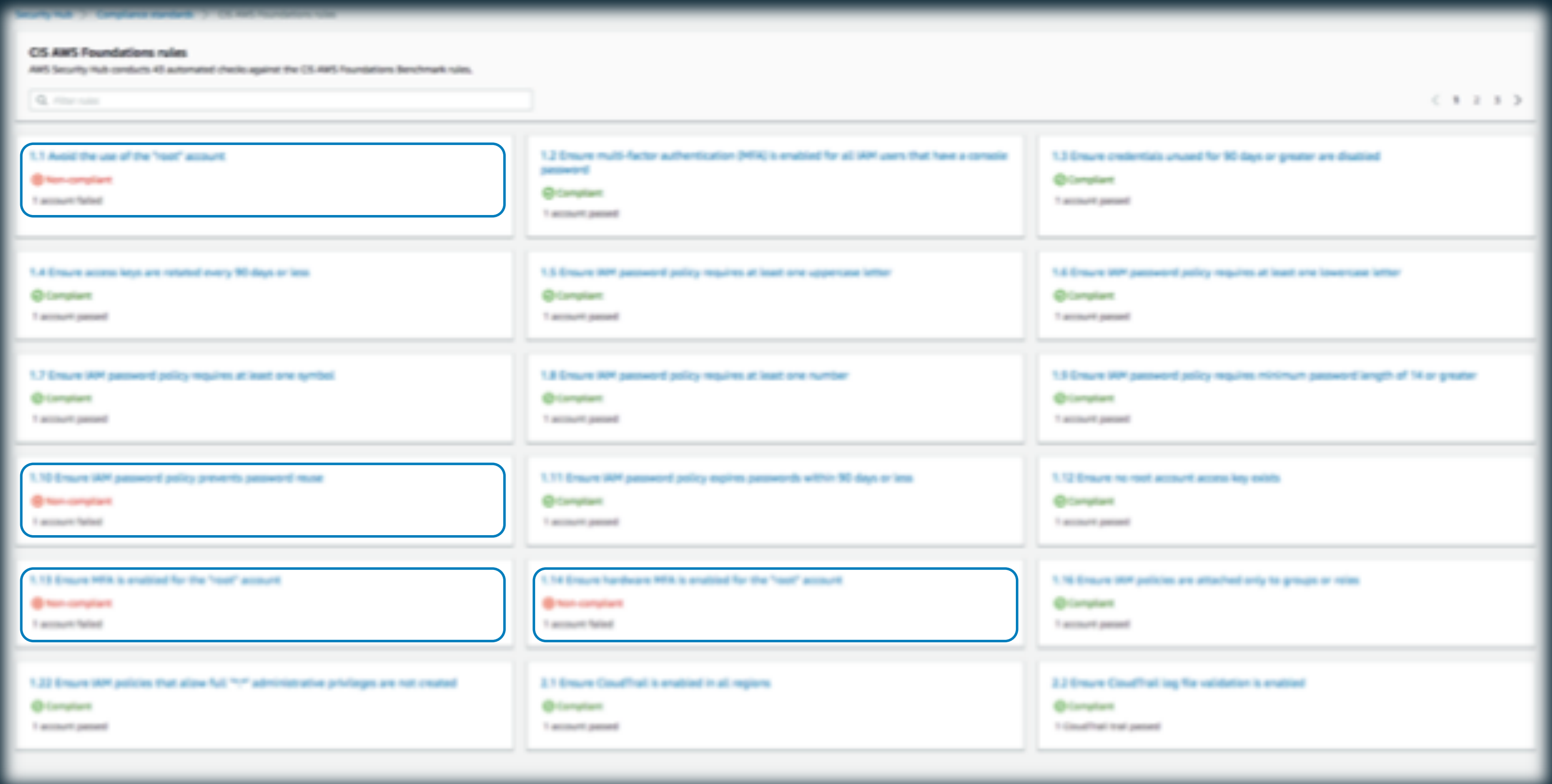
Ensure no Security groups allow ingress from 0.0.0.0/0 to **port 22**

Ensure IAM policies that allow full "*:*" administrative privileges are not created

43 pre configured rules for CIS

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Compliance Standards



Security Hub > Compliance standards > CIS AWS Foundations rules

CIS AWS Foundations rules

AWS Security Hub conducts 43 automated checks against the CIS AWS Foundations Benchmark rules.

Filter rules

< 1 2 3 >

1.1 Avoid the use of the "root" account
Non-compliant
1 account failed

1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
Compliant
1 account passed

1.3 Ensure credentials unused for 90 days or greater are disabled
Compliant
1 account passed

1.4 Ensure access keys are rotated every 90 days or less
Compliant
1 account passed

1.5 Ensure IAM password policy requires at least one uppercase letter
Compliant
1 account passed

1.6 Ensure IAM password policy requires at least one lowercase letter
Compliant
1 account passed

1.7 Ensure IAM password policy requires at least one symbol
Compliant
1 account passed

1.8 Ensure IAM password policy requires at least one number
Compliant
1 account passed

1.9 Ensure IAM password policy requires minimum password length of 14 or greater
Compliant
1 account passed

1.10 Ensure IAM password policy prevents password reuse
Non-compliant
1 account failed

1.11 Ensure IAM password policy expires passwords within 90 days or less
Compliant
1 account passed

1.12 Ensure no root account access key exists
Compliant
1 account passed

1.13 Ensure MFA is enabled for the "root" account
Non-compliant
1 account failed

1.14 Ensure hardware MFA is enabled for the "root" account
Non-compliant
1 account failed

1.16 Ensure IAM policies are attached only to groups or roles
Compliant
1 account passed

1.22 Ensure IAM policies that allow full "*:*" administrative privileges are not created
Compliant
1 account passed

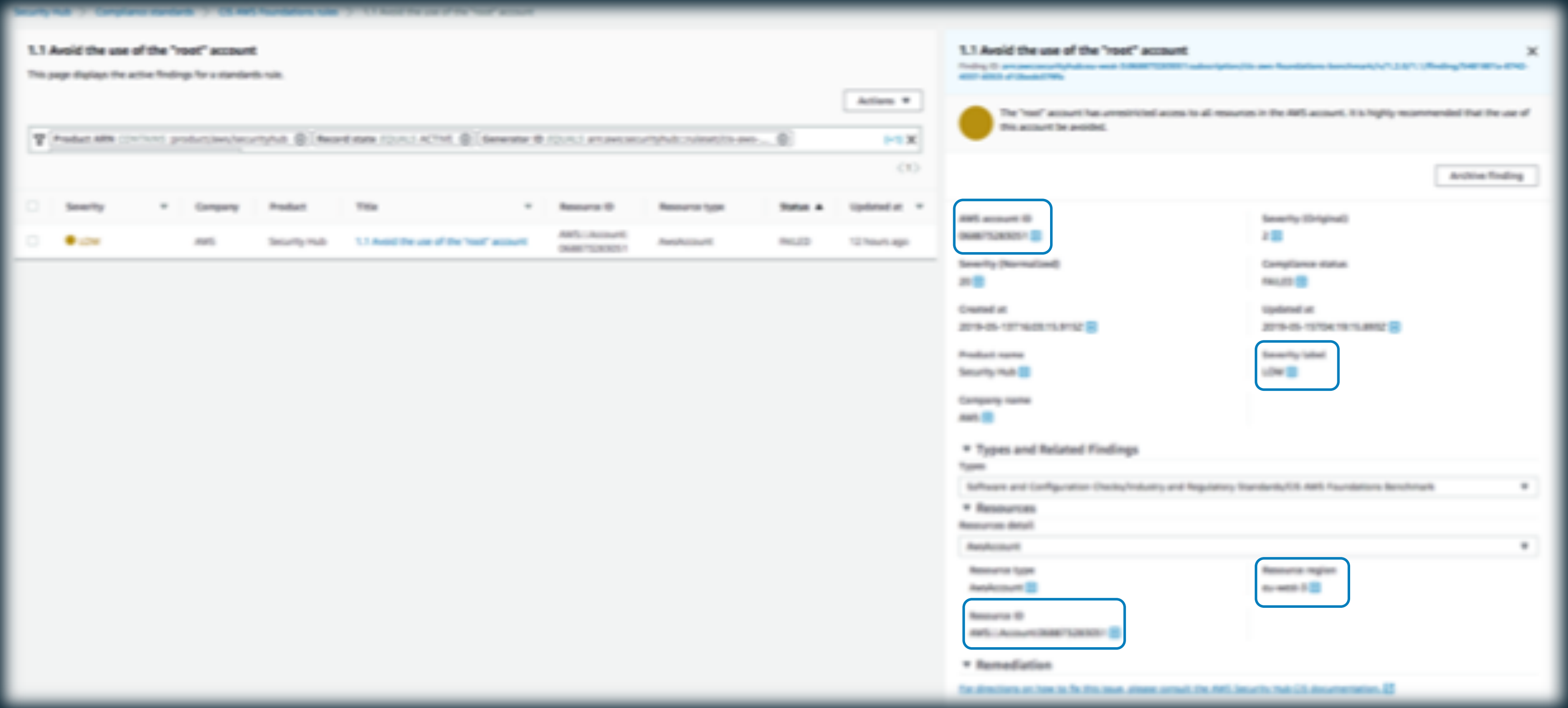
2.1 Ensure CloudTrail is enabled in all regions
Compliant
1 account passed

2.2 Ensure CloudTrail log file validation is enabled
Compliant
1 CloudTrail trail passed

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Compliance Standards

Example: 1.1 Avoid the use of the "root" account



Security Hub > Compliance standards > CIS AWS Foundations rules > 1.1 Avoid the use of the "root" account

1.1 Avoid the use of the "root" account

This page displays the active findings for a standards rule.

Product ARN CONTAINS product/aws/securityhub | Record state EQUALS ACTIVE | Generator ID EQUALS arn:aws:securityhub:::ruleset/cis-aws-...

□	Severity	Company	Product	Title	Resource ID	Resource type	Status ▲	Updated at
□	● LOW	AWS	Security Hub	1.1 Avoid the use of the "root" account	AWS::Account: [illegible]	AwsAccount	FAILED	12 hours ago

1.1 Avoid the use of the "root" account

Finding ID: [illegible]

The "root" account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.

AWS account ID
[illegible]

Severity (Original)
2

Severity (Normalized)
20

Compliance status
FAILED

Created at
2019-05-[illegible]

Updated at
2019-05-[illegible]

Product name
Security Hub

Severity label
LOW

Company name
AWS

▾ Types and Related Findings

Types

Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS Foundations Benchmark

▾ Resources

Resources detail

AwsAccount

Resource type
AwsAccount

Resource region
eu-west-3

Resource ID
AWS::Account:[illegible]

▾ Remediation

For directions on how to fix this issue, please consult the AWS Security Hub CIS documentation.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Security Hub Benefits

Compliance standards

Aggregated findings

Take Action

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Aggregated findings

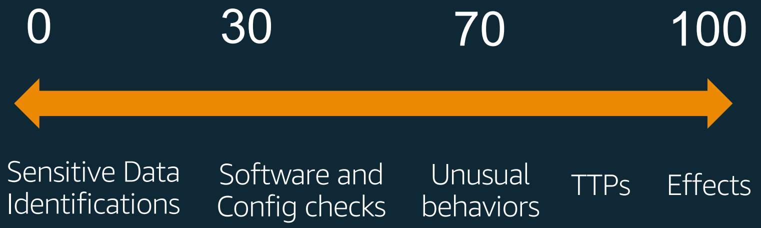
AWS Security Finding Format

~100 JSON-formatted fields

Finding Types

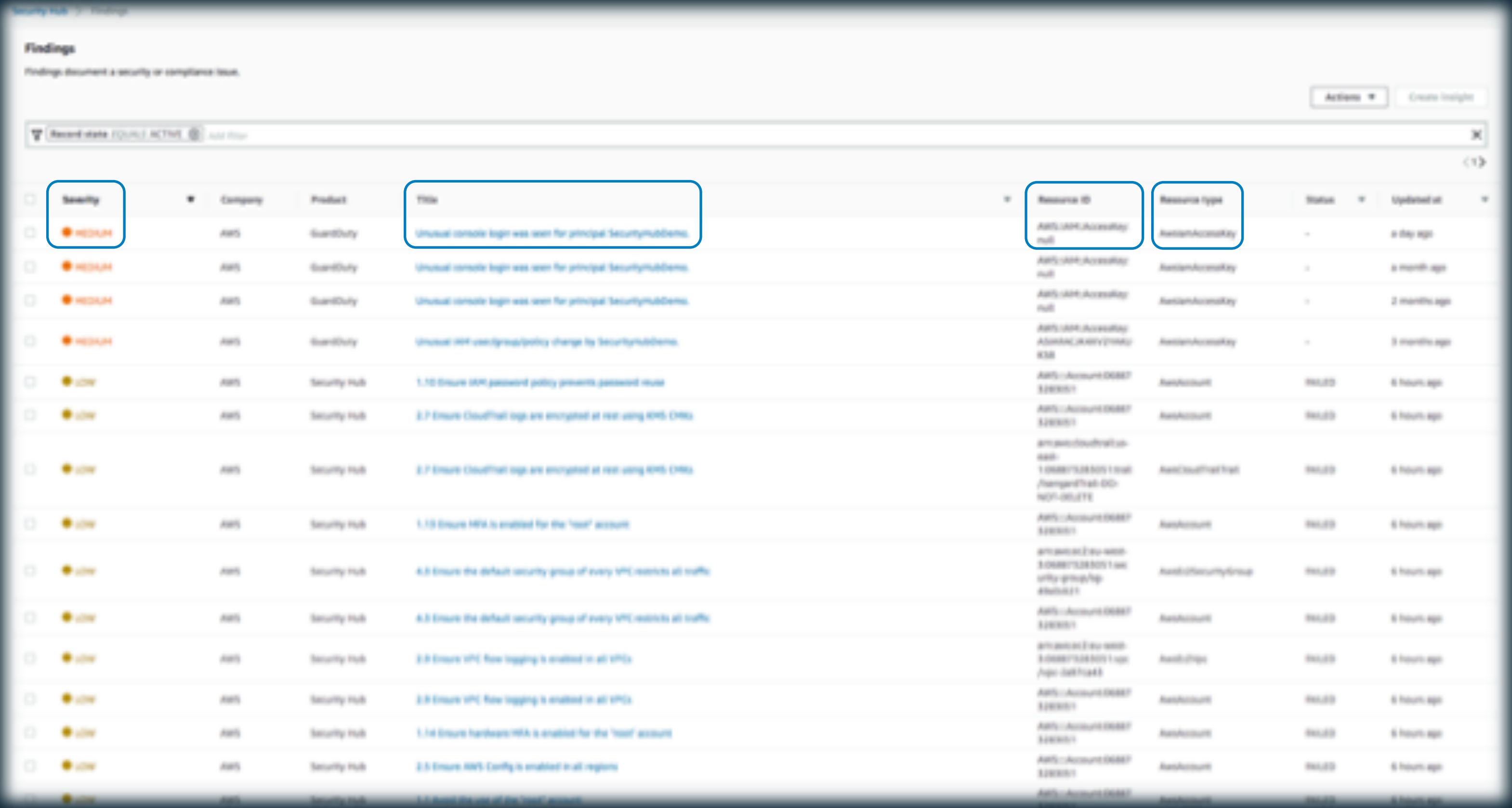
- Sensitive Data Identifications
- Software and Configuration Checks
- Unusual Behaviors
- Tactics, Techniques, and Procedures (TTPs)
- Effects

Severity Normalized



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Aggregated findings



Security Hub > Findings

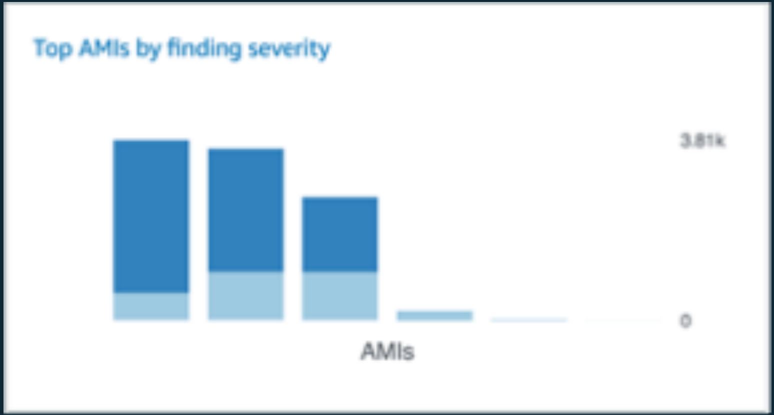
Findings

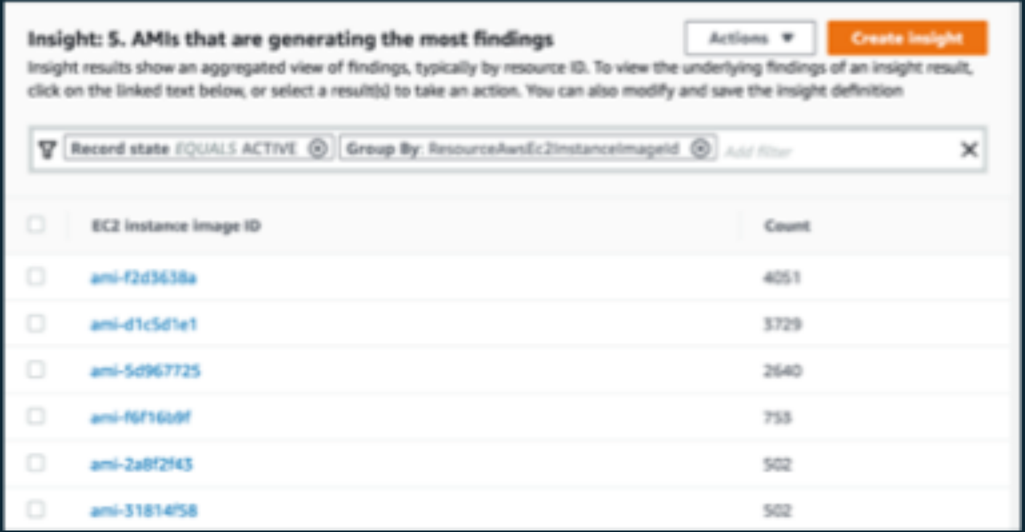
Findings document a security or compliance issue.

□	Severity	Company	Product	Title	Resource ID	Resource type	Status	Updated at
□	● MEDIUM	AWS	GuardDuty	Unusual console login was seen for principal SecurityHubDemo.	AWS::IAM::AccessKey null	AwsIamAccessKey	-	a day ago
□	● MEDIUM	AWS	GuardDuty	Unusual console login was seen for principal SecurityHubDemo.	AWS::IAM::AccessKey null	AwsIamAccessKey	-	a month ago
□	● MEDIUM	AWS	GuardDuty	Unusual console login was seen for principal SecurityHubDemo.	AWS::IAM::AccessKey null	AwsIamAccessKey	-	2 months ago
□	● MEDIUM	AWS	GuardDuty	Unusual IAM user/group/policy change by SecurityHubDemo.	AWS::IAM::AccessKey [illegible]	AwsIamAccessKey	-	3 months ago
□	● LOW	AWS	Security Hub	1.10 Ensure IAM password policy prevents password reuse	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs	arn:aws:cloudtrail:us-east-[illegible]-DO-NOT-DELETE	AwsCloudTrailTrail	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	1.13 Ensure MFA is enabled for the "root" account	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	arn:aws:ec2:eu-west-[illegible]	AwsEc2SecurityGroup	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	4.3 Ensure the default security group of every VPC restricts all traffic	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	2.9 Ensure VPC flow logging is enabled in all VPCs	arn:aws:ec2:eu-west-[illegible]	AwsEc2Vpc	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	2.9 Ensure VPC flow logging is enabled in all VPCs	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	1.14 Ensure hardware MFA is enabled for the "root" account	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	2.5 Ensure AWS Config is enabled in all regions	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago
□	● LOW	AWS	Security Hub	1.1 Avoid the use of the "root" account	AWS::::Account:[illegible]	AwsAccount	FAILED	6 hours ago

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Insights help identify resources that require attention





Insight: 5. AMIs that are generating the most findings

Insight results show an aggregated view of findings, typically by resource ID. To view the underlying findings of an insight result, click on the linked text below, or select a result(s) to take an action. You can also modify and save the insight definition

Record state EQUALS ACTIVE ⊗ Group By: ResourceAwsEc2InstanceImageId ⊗

□	EC2 instance image ID	Count
□	ami-f2d3638a	4051
□	ami-d1c5d1e1	3729
□	ami-5d967725	2640
□	ami-f6f16b9f	753
□	ami-2a8f2f43	502
□	ami-31814f58	502

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Security Hub insights

- Dashboard provides visibility into the top security findings
- 20 pre-built insights provided by AWS and AWS partners
- Customer can create their own insights

- Examples:

EC2 instances that have missing security patches

S3 buckets with stored credentials

S3 buckets with public read and write permissions

Top AMIs by counts of findings

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Security Hub Benefits

Compliance standards

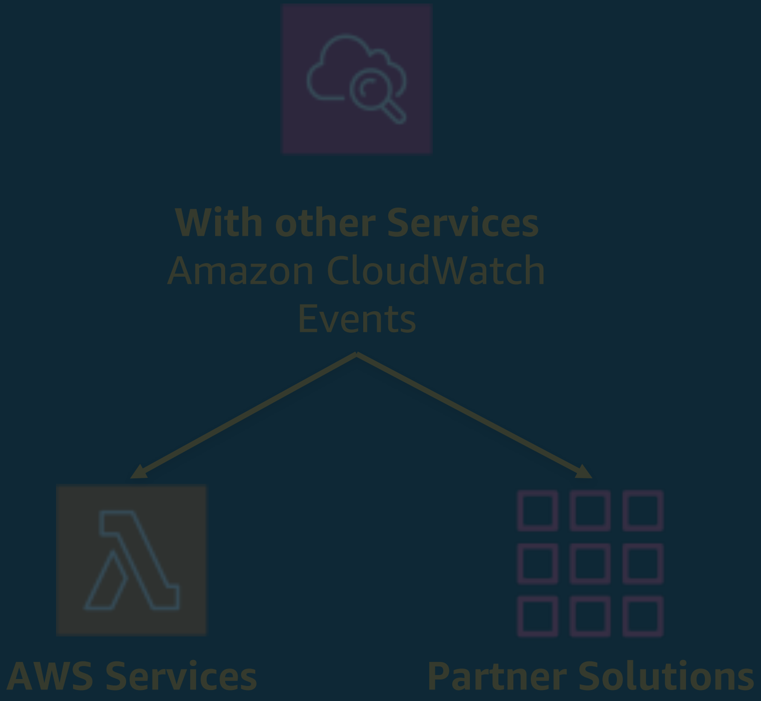
Aggregated findings

Take Action

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Take Action

Custom Actions
Amazon Security Hub



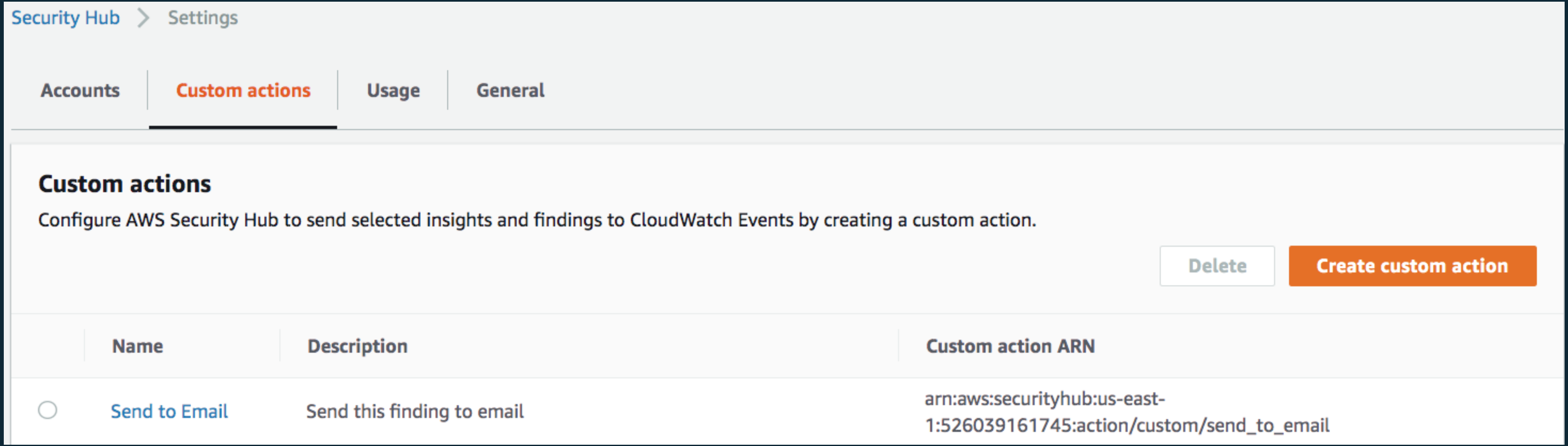
With other Services
Amazon CloudWatch Events

AWS Services

Partner Solutions

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Custom Actions in Security Hub



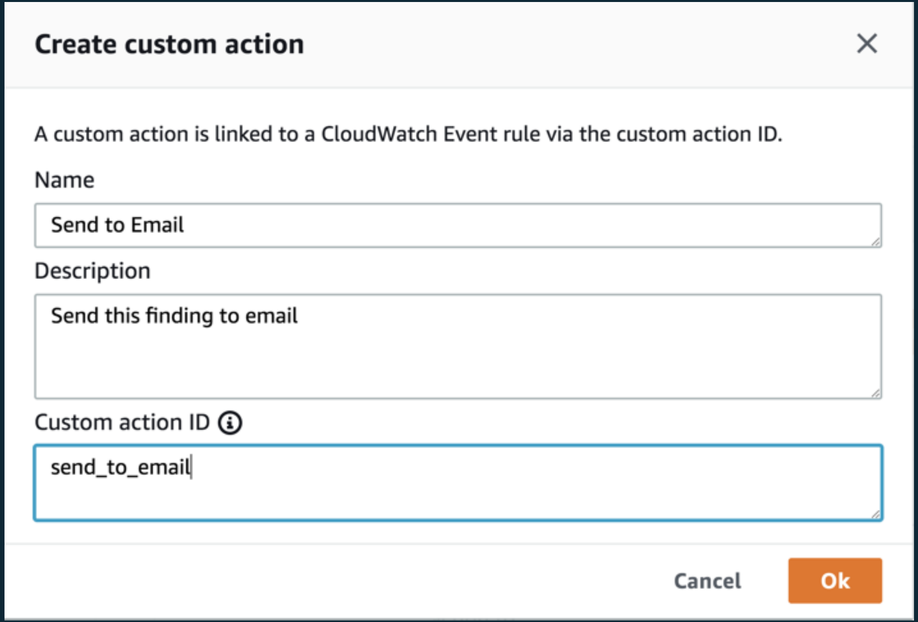
Custom actions

Configure AWS Security Hub to send selected insights and findings to CloudWatch Events by creating a custom action.

	Name	Description	Custom action ARN
○	Send to Email	Send this finding to email	arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_email

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Custom Actions in Security Hub



Create custom action

A custom action is linked to a CloudWatch Event rule via the custom action ID.

Name

Send to Email

Description

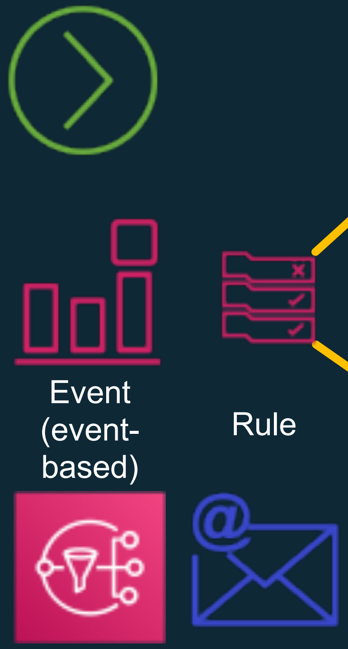
Send this finding to email

Custom action ID

send_to_email

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

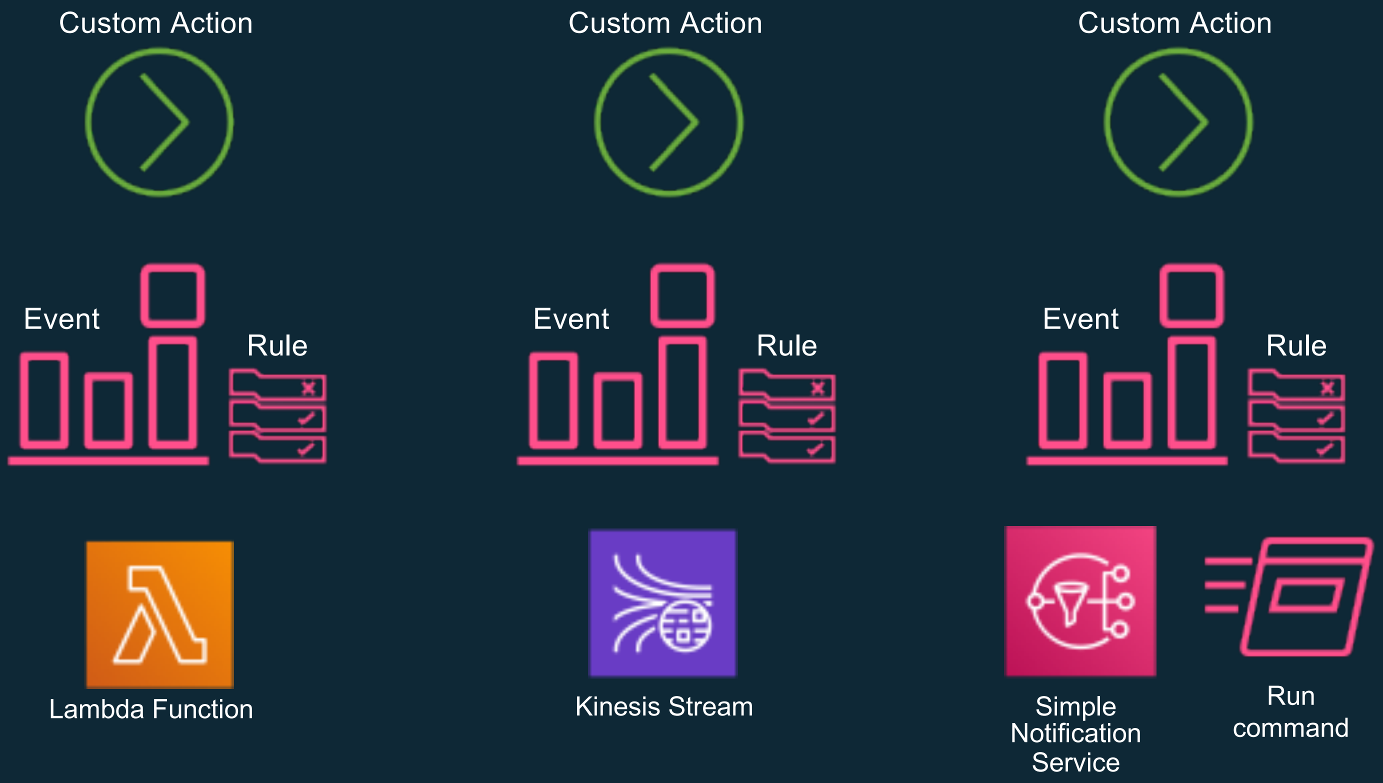
Custom Actions in Security Hub



```
{
  "source": [
    "aws.securityhub"
  ],
  "resources": [
    "arn:aws:securityhub:us-west-
2:xxxxxxxxxxxx:action/custom/send_to
_email"
  ]
}
```

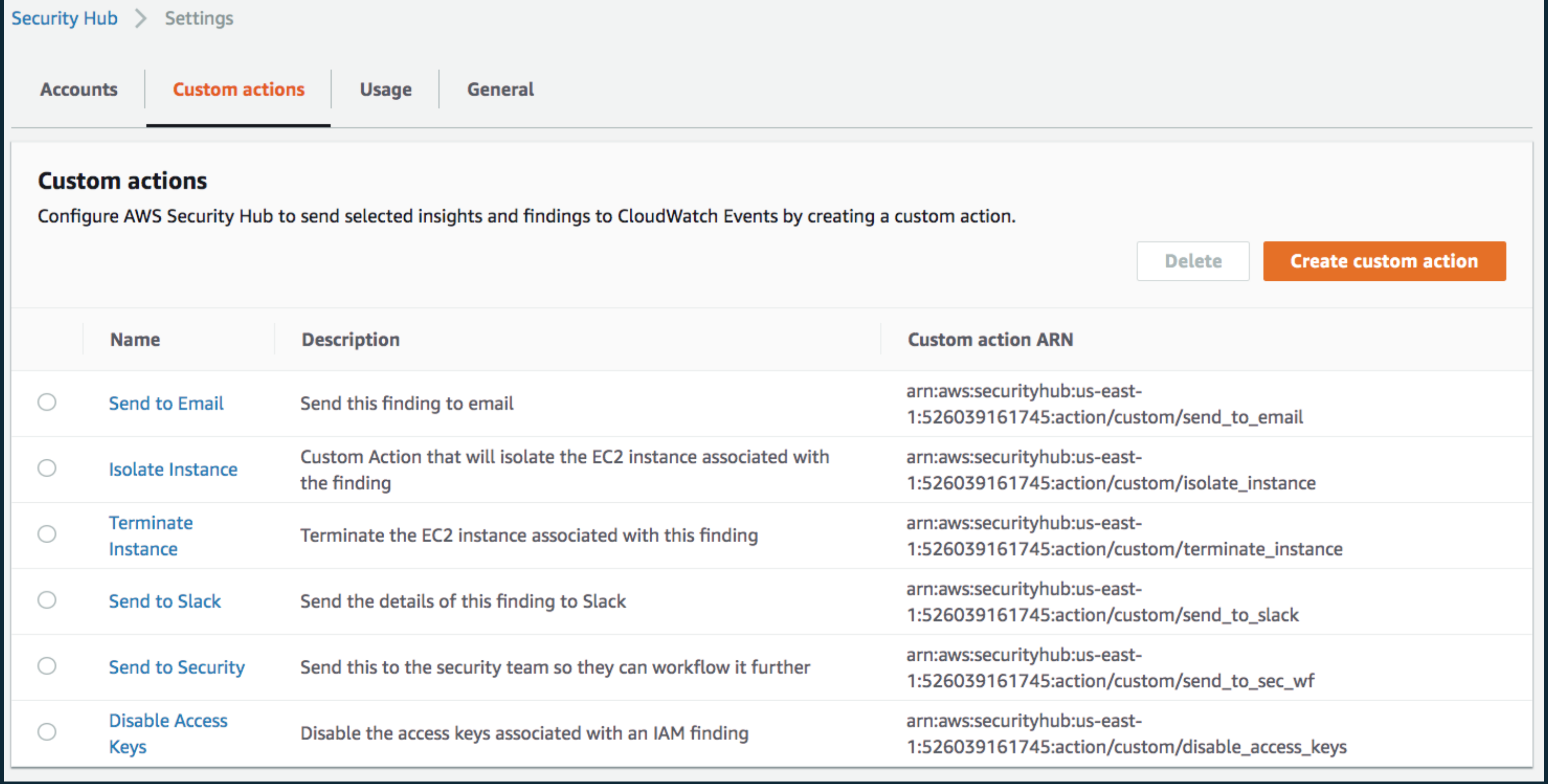
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Custom Actions in Security Hub



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Custom Actions in Security Hub



Custom actions

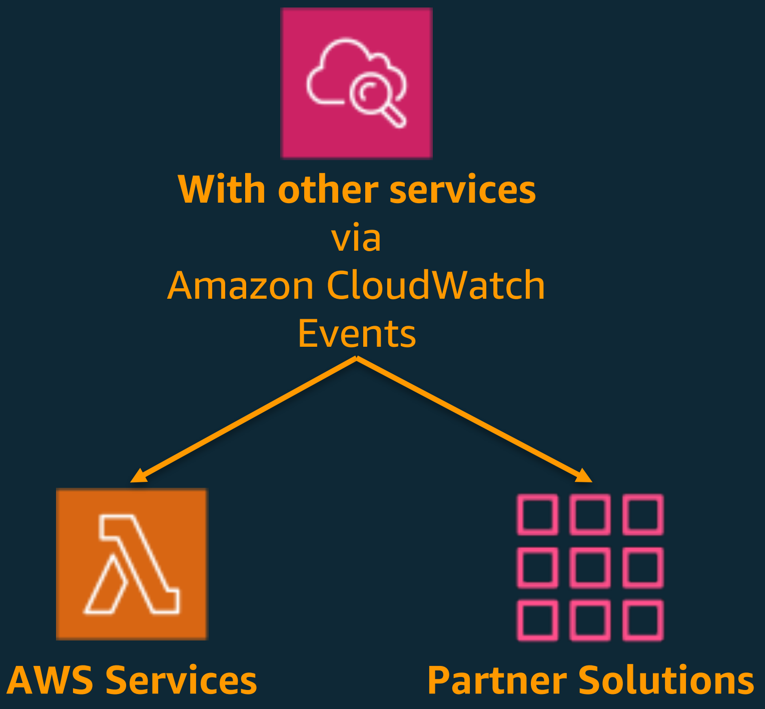
Configure AWS Security Hub to send selected insights and findings to CloudWatch Events by creating a custom action.

	Name	Description	Custom action ARN
○	Send to Email	Send this finding to email	arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_email
○	Isolate Instance	Custom Action that will isolate the EC2 instance associated with the finding	arn:aws:securityhub:us-east-1:526039161745:action/custom/isolate_instance
○	Terminate Instance	Terminate the EC2 instance associated with this finding	arn:aws:securityhub:us-east-1:526039161745:action/custom/terminate_instance
○	Send to Slack	Send the details of this finding to Slack	arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_slack
○	Send to Security	Send this to the security team so they can workflow it further	arn:aws:securityhub:us-east-1:526039161745:action/custom/send_to_sec_wf
○	Disable Access Keys	Disable the access keys associated with an IAM finding	arn:aws:securityhub:us-east-1:526039161745:action/custom/disable_access_keys

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Take Action

Custom Actions
via
Amazon Security
Hub



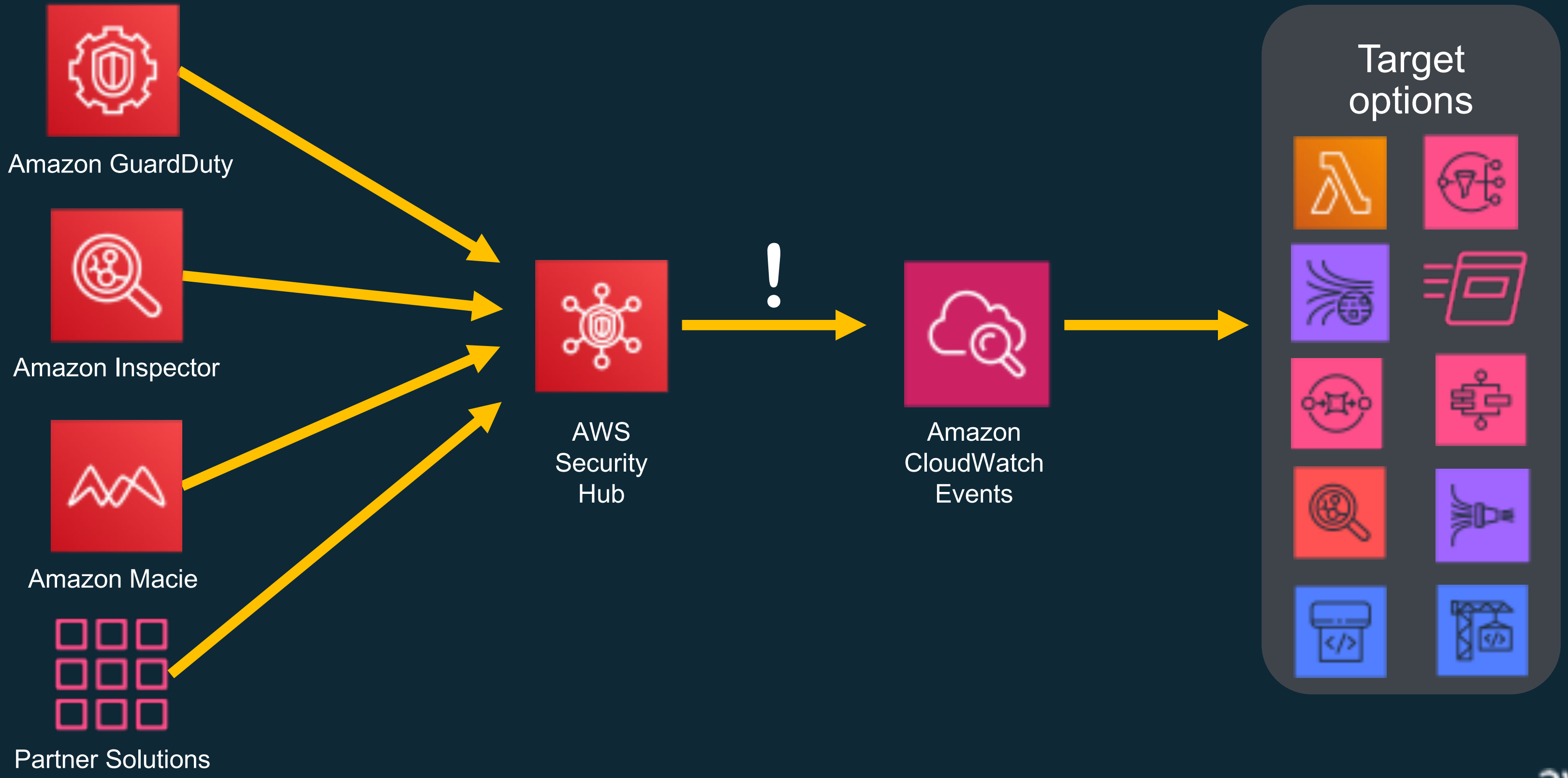
With other services
via
Amazon CloudWatch
Events

AWS Services

Partner Solutions

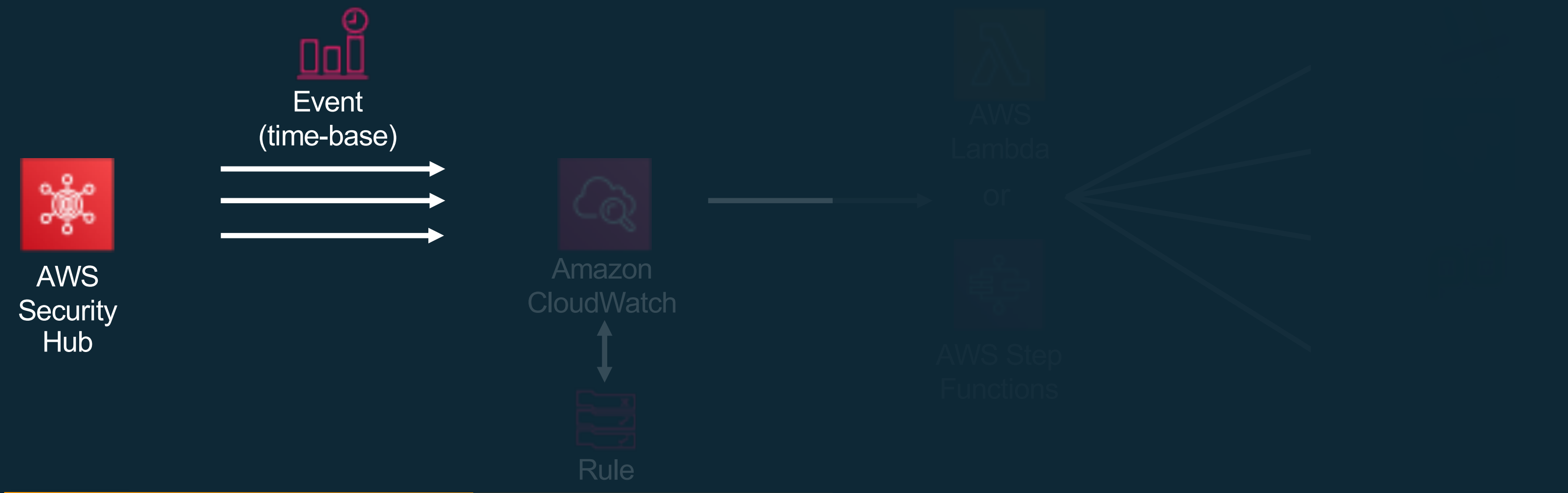
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Taking Action with Security Hub partner



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Customizable response and remediation actions



1. All findings automatically send to CloudWatch events; AND

2. AWS Security Hub user selects findings in the console and takes a custom action on them. These findings are sent to CloudWatch decorated with a custom action ID

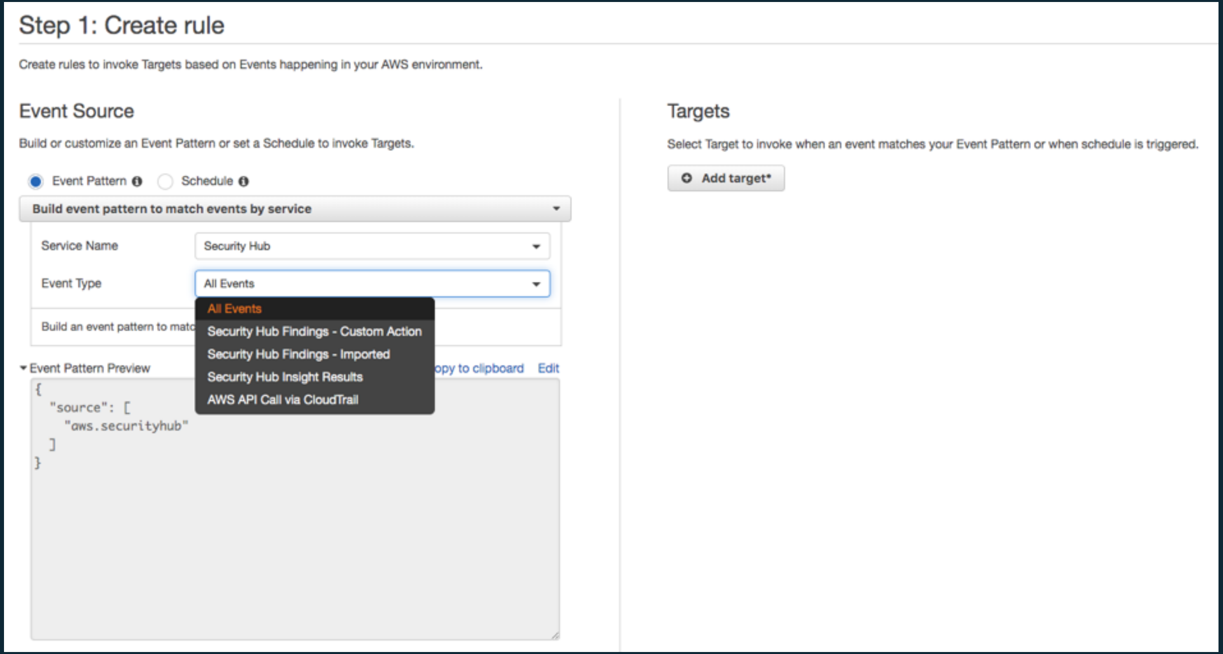
3. User creates CloudWatch event rules to look for certain findings associated with a custom action id or types of findings.

4. The rule defines a target – typically a Lambda function, Step Function, or Automation document

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Taking Action on All Findings

Every new Security Hub finding is sent to Amazon CloudWatch Events



Step 1: Create rule

Create rules to invoke Targets based on Events happening in your AWS environment.

Event Source

Build or customize an Event Pattern or set a Schedule to invoke Targets.

● Event Pattern ○ Schedule

Build event pattern to match events by service

Service Name: Security Hub

Event Type: All Events

Build an event pattern to matc

Event Pattern Preview

```
{
  "source": [
    "aws.securityhub"
  ]
}
```

All Events
Security Hub Findings - Custom Action
Security Hub Findings - Imported
Security Hub Insight Results
AWS API Call via CloudTrail
opy to clipboard
Edit

Targets

Select Target to invoke when an event matches your Event Pattern or when schedule is triggered.

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Event Pattern Examples

Filter by Tags

```
{
  “source”: [
    “aws.securityhub”
  ],
  “detail-type”: [
    “Security Hub Findings”
  ],
  “detail”: {
    “findings”: {
      “Resources”: {
        “Tags”: {
          “Environment”: [
            “PCI”
          ]
        }
     }
      }
     }
    }
```

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Event Pattern Examples

Filter by Severity

```
{
  “source”: [
    “aws.securityhub”
  ],
  “detail-type”: [
    “Security Hub Findings”
  ],
  “detail”: {
    “findings”: {
      “Severity”: {
        “Normalized”: [
          95,
          96,
          97,
          98,
          99,
          100
        ]
      }}}}
```

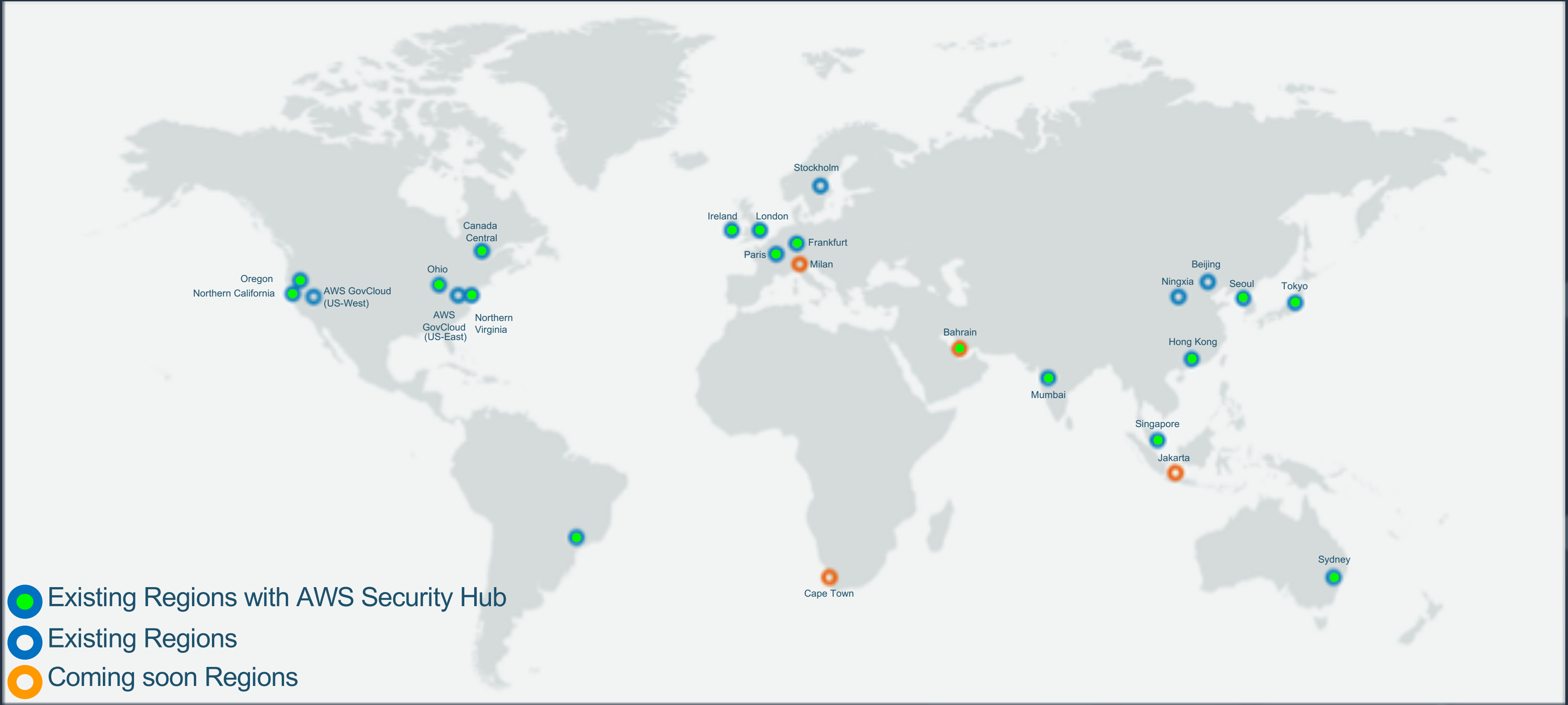
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Services Availability

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

AWS Security Hub

Services Availability (Regions)



© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Pricing

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Pricing

- Free trial: All AWS accounts will have a **30-day free trial**.

Finding ingestion pricing:

- **Free tier:** Post 30 days, a perpetual free tier of 10,000 findings ingestion events per account per month.
- Then - finding ingestion events are $0.3 per 10,000 findings.

Events	Pricing
First 10,000 events / month	Free
10,001 + events / month	$0.00003/finding

Compliance Standards pricing:

Charge is based on the following:

- Per compliance check
- Per AWS account
- Per region
- Per month

Compliance Standards	Pricing
First 100,000	$0.0010/check
100,001-500,000	$0.0008/check
500,001+	$0.0005/check

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Reference Customers

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Reference Customers

airbnb
edmunds
intuit.
Frame.io
GoDaddy
here
COMCAST
THOMSON REUTERS®
move

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Use Case 1:

Centralized security and compliance workspace

Goal	**Have a single pane of glass to view, triage, and take action on AWS security and compliance issues across accounts**
Personas	SecOps, compliance, and/or DevSecOps teams focused on AWS, Cloud Centers of Excellence, the first security hire
Key processes example	1. Ingest findings from finding providers 2. High-volume and well-known findings are programmatically routed to remediation workflows, which include updating the status of the finding 3. Remaining findings are routed to analysts via an on-call management system, and they use ticketing and chat systems to resolve them
Taking action integrations	Ticketing systems, chat systems, on-call management systems, SOAR platforms, customer-built remediation playbooks

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use pattern 2:
Centralized routing to a SIEM

Goal	**Easily route all AWS security and compliance findings in a normalized format to a centralized SIEM or log management tool**
Personas	SecOps, compliance, and/or DevSecOps teams
Key processes example	1. Ingest findings from finding providers 2. All findings are routed via Amazon CloudWatch Events to a central SIEM that stores AWS and on-premises security and compliance data 3. Analyst workflows are linked to the central SIEM
Taking action integrations	SIEM

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use pattern 3:
Dashboard for account owners

Goal	**Provide visibility to AWS account owners on the security and compliance posture of their account**
Personas	AWS account owners
Key processes example	1. Ingest findings from finding providers 2. Account owners are given read-only access to Security Hub 3. Account owners can use Security Hub to research issues that they are ticketed on or proactively monitor their own security and compliance state
Taking action integrations	Chat, ticketing

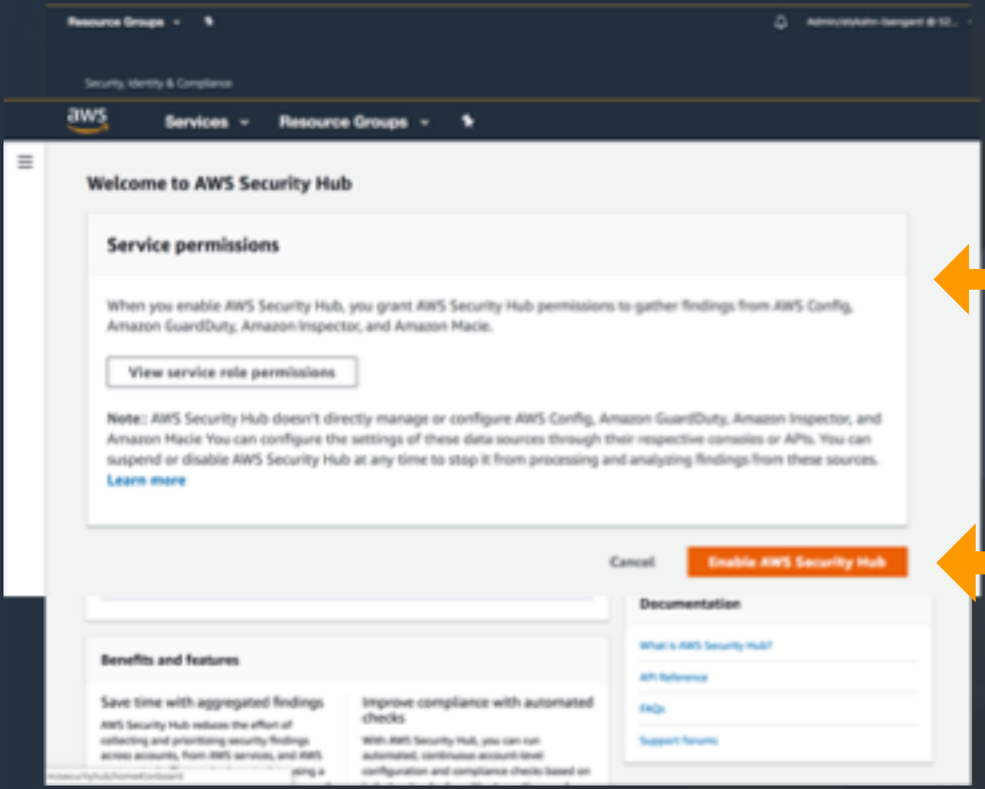
© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Getting Started

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Getting Started

A few clicks to enable Security Hub


Resource Groups
Security, Identity & Compliance
aws
Services
Resource Groups

Welcome to AWS Security Hub

Service permissions

When you enable AWS Security Hub, you grant AWS Security Hub permissions to gather findings from AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie.

View service role permissions

Note:: AWS Security Hub doesn't directly manage or configure AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable AWS Security Hub at any time to stop it from processing and analyzing findings from these sources. Learn more

Benefits and features

Save time with aggregated findings

AWS Security Hub reduces the effort of collecting and prioritizing security findings across accounts, from AWS services, and AWS

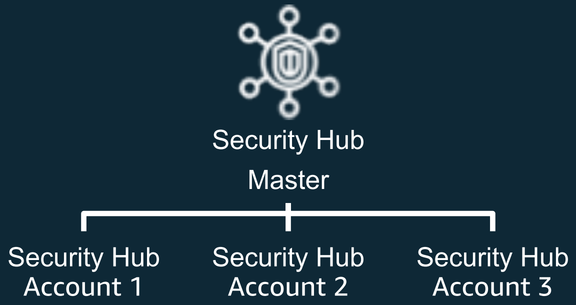
Improve compliance with automated checks

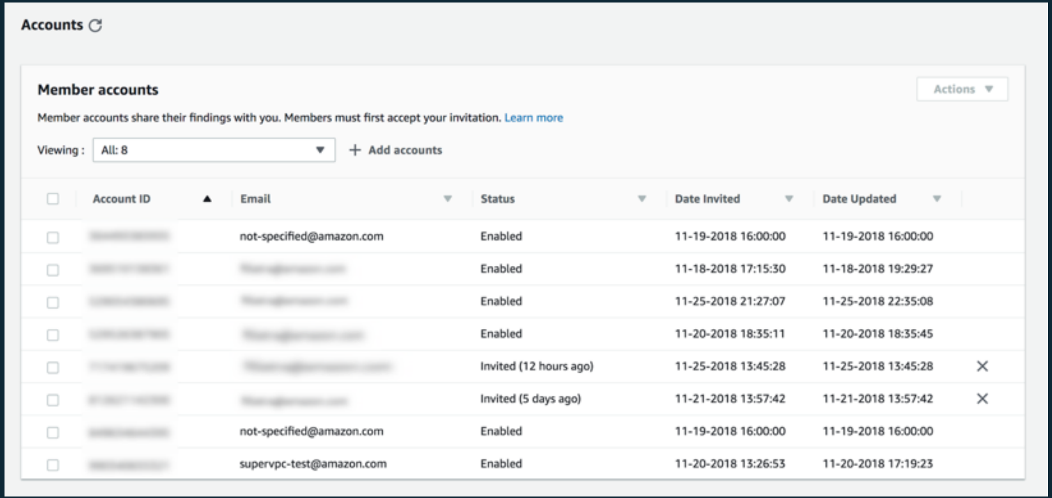
With AWS Security Hub, you can run automated, continuous account-level configuration and compliance checks based on

Documentation

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Simple multi-account setup





Accounts

Member accounts

Member accounts share their findings with you. Members must first accept your invitation. Learn more

Viewing : All: 8

□	Account ID ▲	Email	Status	Date Invited	Date Updated	
□	[redacted]	not-specified@amazon.com	Enabled	11-19-2018 16:00:00	11-19-2018 16:00:00	
□	[redacted]	[redacted]	Enabled	11-18-2018 17:15:30	11-18-2018 19:29:27	
□	[redacted]	[redacted]	Enabled	11-25-2018 21:27:07	11-25-2018 22:35:08	
□	[redacted]	[redacted]	Enabled	11-20-2018 18:35:11	11-20-2018 18:35:45	
□	[redacted]	[redacted]	Invited (12 hours ago)	11-25-2018 13:45:28	11-25-2018 13:45:28	✕
□	[redacted]	[redacted]	Invited (5 days ago)	11-21-2018 13:57:42	11-21-2018 13:57:42	✕
□	[redacted]	not-specified@amazon.com	Enabled	11-19-2018 16:00:00	11-19-2018 16:00:00	
□	[redacted]	supervpc-test@amazon.com	Enabled	11-20-2018 13:26:53	11-20-2018 17:19:23	

Learn more about
AWS Landing Zone Solution

Bulk enable Security Hub across multiple accounts you control using this multi-account enable script
Multi-account enable script

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

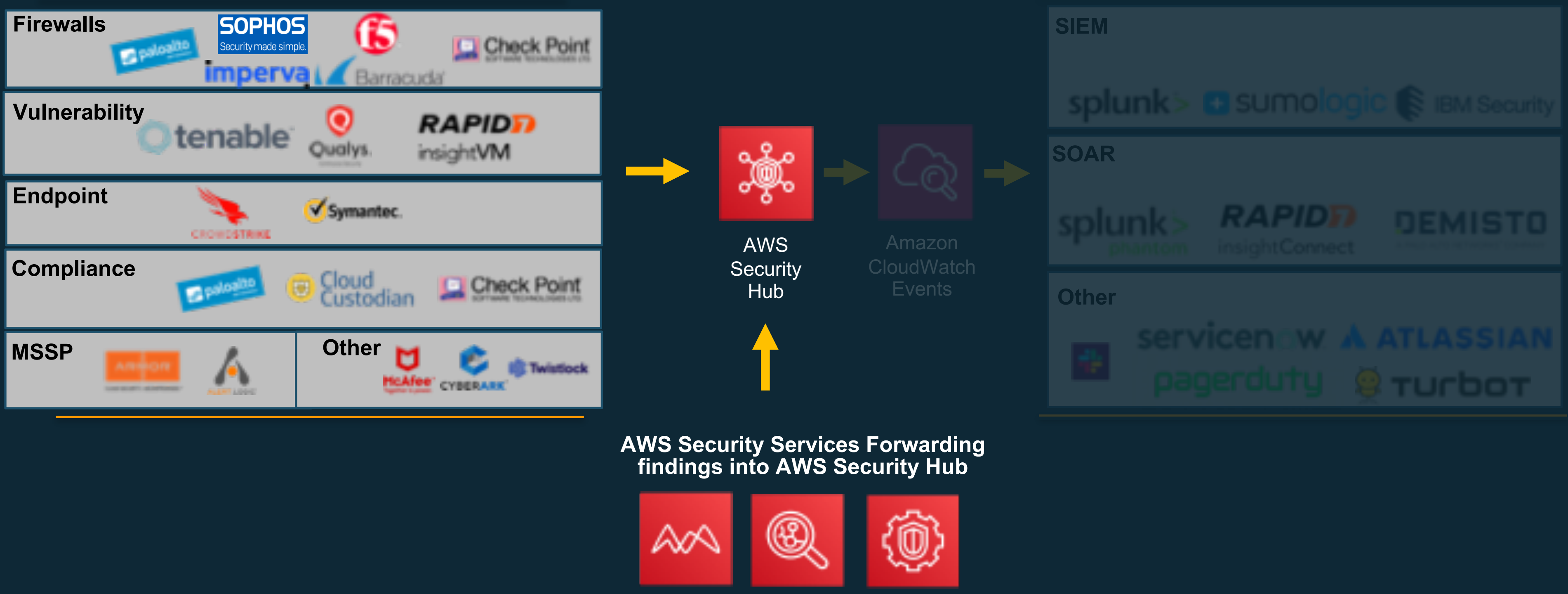
Partner integrations

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Partner integrations

Partners forwarding findings into AWS Security Hub

"Taking Action"



AWS Security Hub

Amazon CloudWatch Events

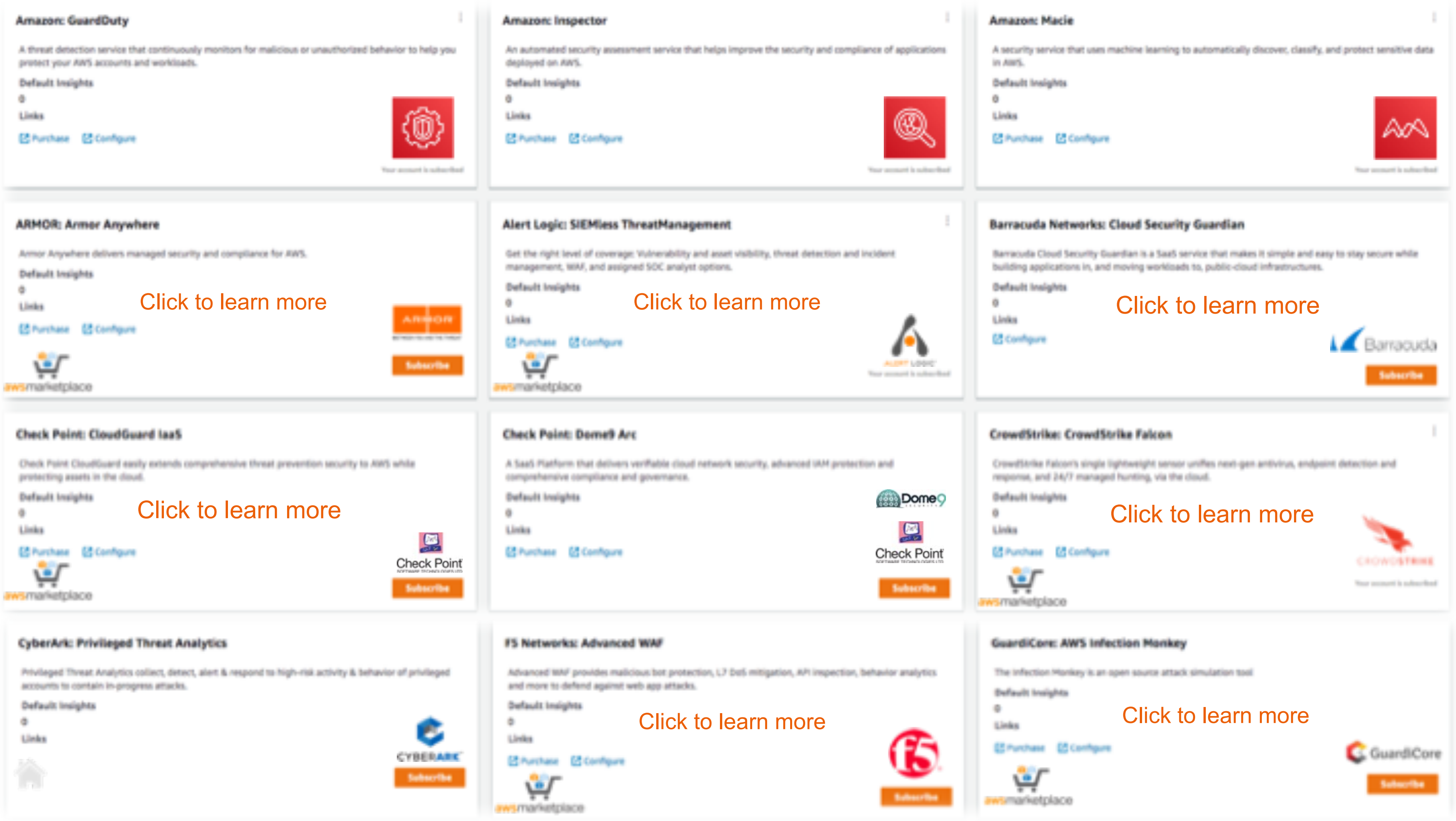
AWS Security Services Forwarding findings into AWS Security Hub

Amazon Macie

Amazon Inspector

Amazon GuardDuty

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



Amazon: GuardDuty

A threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads.

Default Insights

0

Links

Purchase Configure

Your account is subscribed

Amazon: Inspector

An automated security assessment service that helps improve the security and compliance of applications deployed on AWS.

Default Insights

0

Links

Purchase Configure

Your account is subscribed

Amazon: Macie

A security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS.

Default Insights

0

Links

Purchase Configure

Your account is subscribed

ARMOR: Armor Anywhere

Armor Anywhere delivers managed security and compliance for AWS.

Default Insights

0

Links

Purchase Configure

Click to learn more

Subscribe

awsmarketplace

Alert Logic: SIEMless ThreatManagement

Get the right level of coverage: Vulnerability and asset visibility, threat detection and incident management, WAF, and assigned SOC analyst options.

Default Insights

0

Links

Purchase Configure

Click to learn more

Your account is subscribed

awsmarketplace

Barracuda Networks: Cloud Security Guardian

Barracuda Cloud Security Guardian is a SaaS service that makes it simple and easy to stay secure while building applications in, and moving workloads to, public-cloud infrastructures.

Default Insights

0

Links

Configure

Click to learn more

Subscribe

Check Point: CloudGuard IaaS

Check Point CloudGuard easily extends comprehensive threat prevention security to AWS while protecting assets in the cloud.

Default Insights

0

Links

Purchase Configure

Click to learn more

Subscribe

awsmarketplace

Check Point: Dome9 Arc

A SaaS Platform that delivers verifiable cloud network security, advanced IAM protection and comprehensive compliance and governance.

Default Insights

0

Links

Purchase Configure

Subscribe

CrowdStrike: CrowdStrike Falcon

CrowdStrike Falcon's single lightweight sensor unifies next-gen antivirus, endpoint detection and response, and 24/7 managed hunting, via the cloud.

Default Insights

0

Links

Purchase Configure

Click to learn more

Your account is subscribed

awsmarketplace

CyberArk: Privileged Threat Analytics

Privileged Threat Analytics collect, detect, alert & respond to high-risk activity & behavior of privileged accounts to contain in-progress attacks.

Default Insights

0

Links

Subscribe

F5 Networks: Advanced WAF

Advanced WAF provides malicious bot protection, L7 DoS mitigation, API inspection, behavior analytics and more to defend against web app attacks.

Default Insights

0

Links

Purchase Configure

Click to learn more

Subscribe

awsmarketplace

GuardiCore: AWS Infection Monkey

The Infection Monkey is an open source attack simulation tool

Default Insights

0

Links

Purchase Configure

Click to learn more

Subscribe

awsmarketplace

Key takeaways

- Automatically evaluate your compliance against key standards with one-click, frictionless enablement
- Centralize all of your findings via the AWS Security Findings Format without the need to parse and normalize them
- Prioritize findings using insights for efficient response and remediation
- Take actions on findings automatically or semi-automatically using CloudWatch events
- View and understand your security and compliance state in one place

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Thank you!

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.