

Hands-on with AWS Security Hub

Agenda

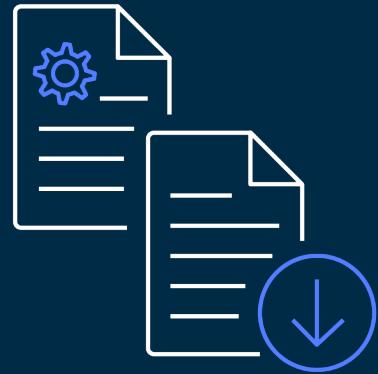
Security Hub Overview

Inbound Integrations

Outbound Integrations – Taking action

Workshop details

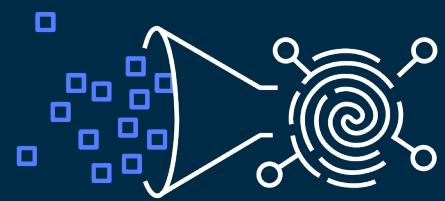
Security and Compliance Challenges



Backlog of
Compliance
requirements



Complexity

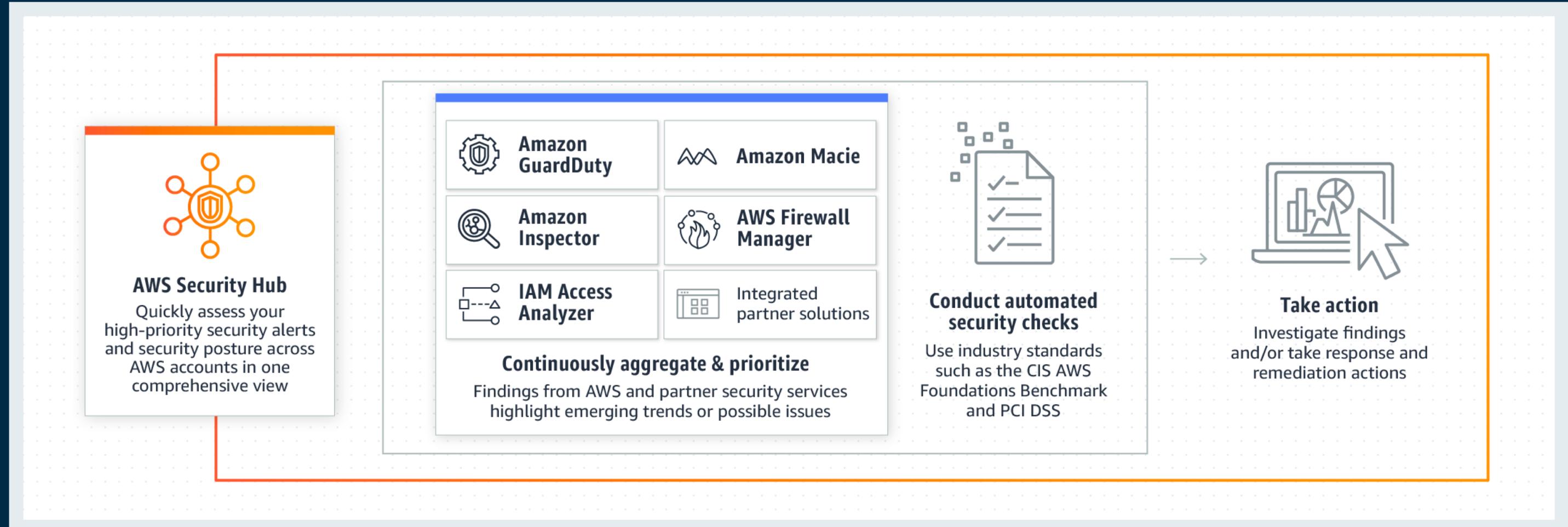


Signal to
Noise Ratio



Lack of an
Integrated View

Security Hub overview



Partner integrations

Firewalls

SOPHOS
Security made simple.



imperva



Vulnerability



RAPID7

SOAR

DEMISTO



TURBOT

SIEM



IBM Security

splunk®

Endpoint



Compliance



MSSP



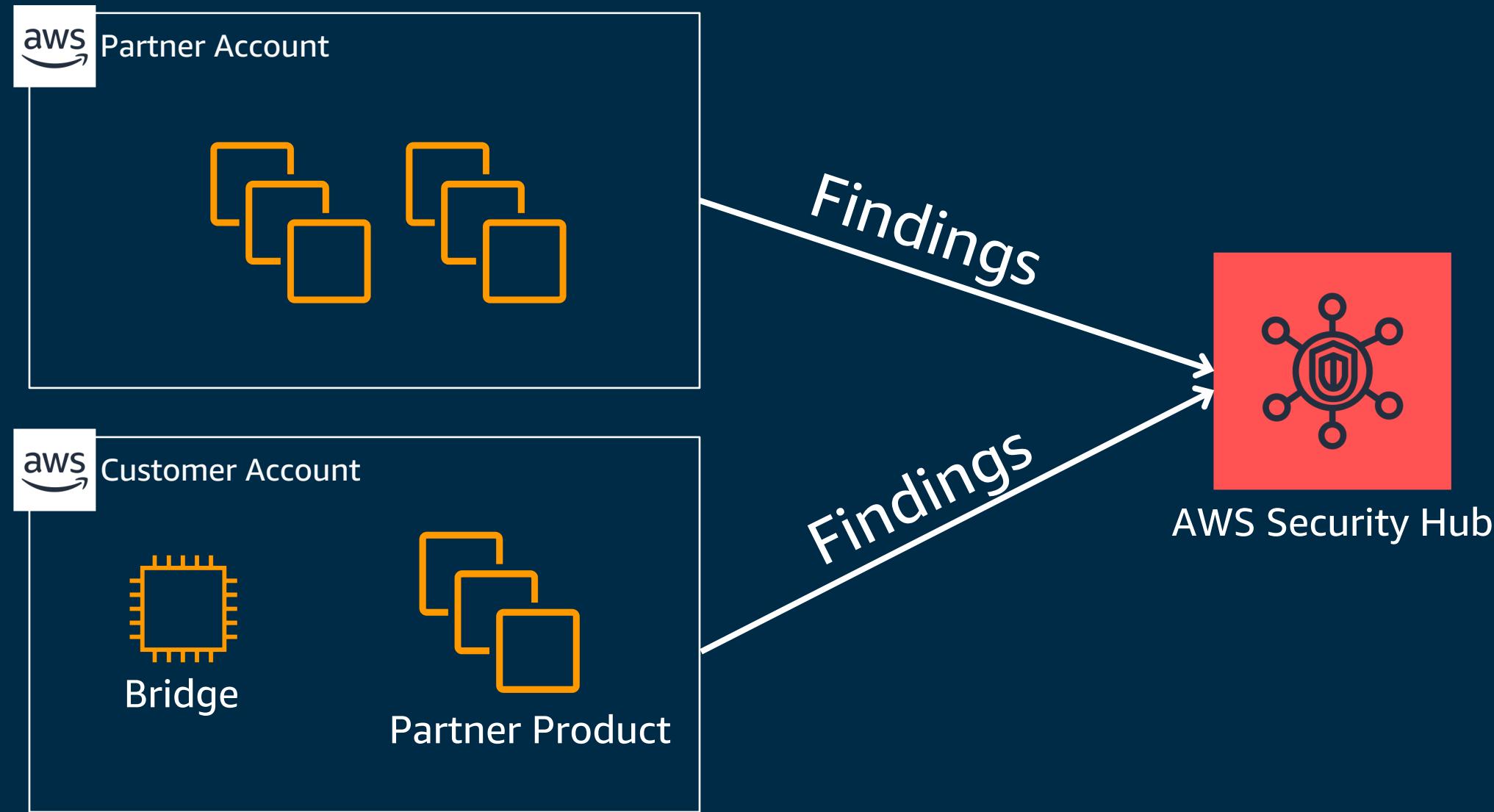
CLOUD SECURITY, UNCOMPROMISED.™



Other



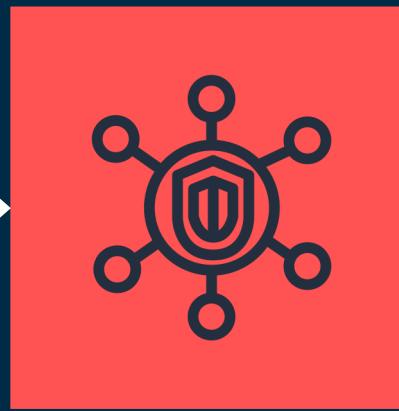
Partner integrations – into Security Hub



You can create your own findings



Your Code



AWS Security Hub

Setup and multi-account

The screenshot shows the AWS Accounts page with the title "Accounts" at the top left. Below it, a section titled "Member accounts" displays a list of 8 accounts. The list includes columns for Account ID, Email, Status, Date Invited, and Date Updated. The "Actions" button is located at the top right of the list. The accounts listed are:

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

Security and Compliance checks

Security Hub X

Security Hub > Security standards

Security standards

New **AWS Foundational Security Best Practices v1.0.0** by AWS

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



71%

Disable View results

CIS AWS Foundations Benchmark v1.2.0 by AWS

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



26%

Disable View results

PCI DSS v3.2.1 by AWS

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

Findings

Security Hub > Findings

Findings

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

Record state EQUALS ACTIVE X Add filters

Actions ▾ Create insight

< 1 ... >

Severity
<input type="checkbox"/> LOW
<input checked="" type="checkbox"/> LOW

Findings

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

Severity label EQUALS CRITICAL X Workflow status EQUALS NEW X

Workflow status EQUALS NOTIFIED X Record state EQUALS ACTIVE X Add filters

Actions ▾ Change workflow status ▾ Create insight

< 1 >

Severity	Workflow status	Company	Product	Title	Resource ID
<input checked="" type="checkbox"/> CRITICAL	NEW	AWS	Security Hub	1.1 Avoid the use of the "root" account	AWS:::Account: [REDACTED]

1.1 Avoid the use of the "root" account

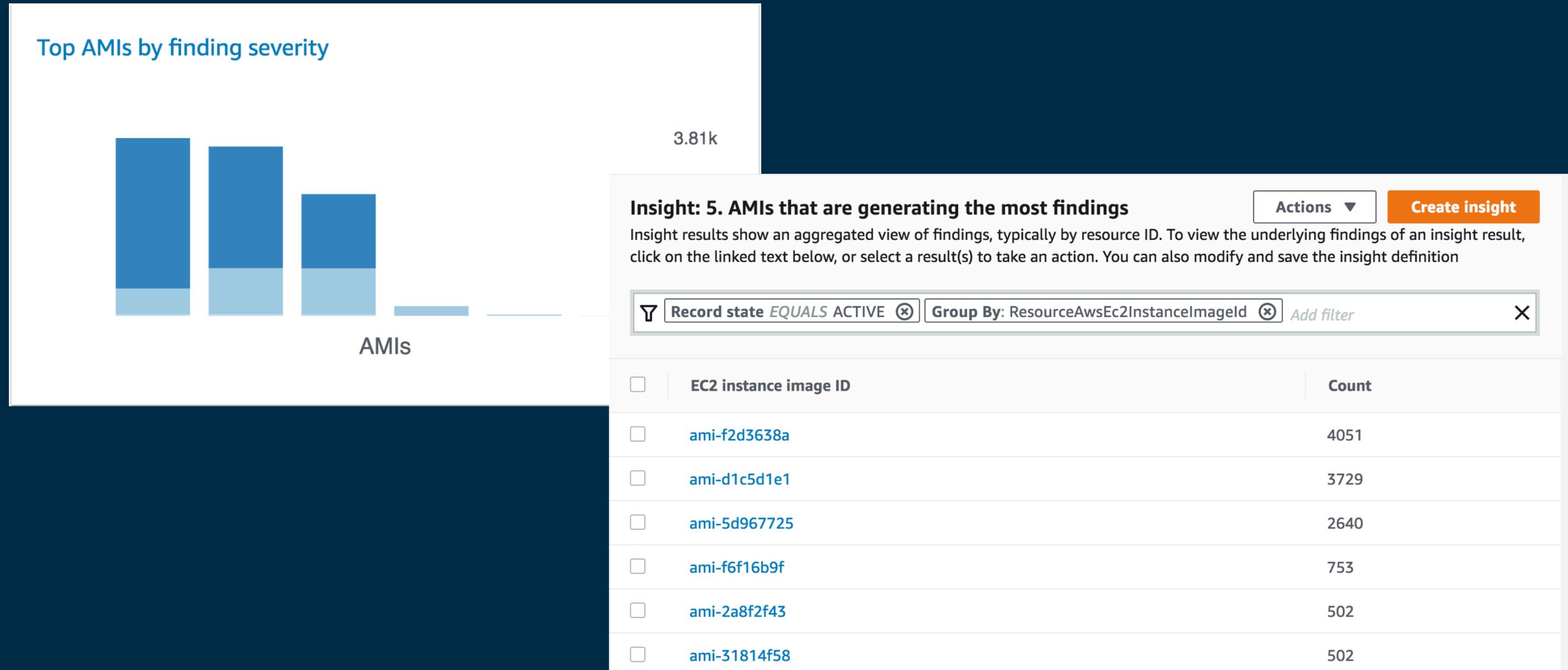
Finding ID: arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0/1.1/finding/e022f8b1-f7e3-407b-ad91-dd3c90b377e7

CRITICAL

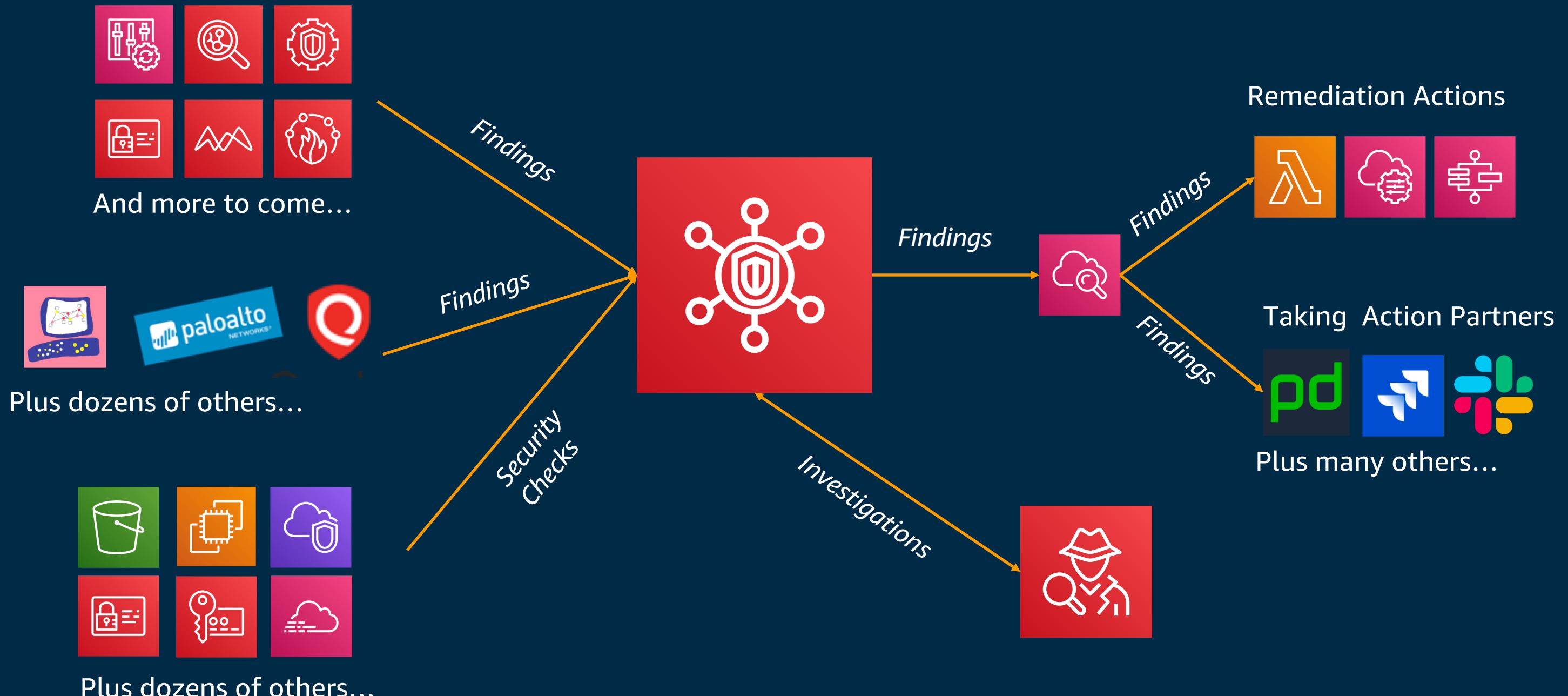
The "root" account has unrestricted access to all resources in the AWS account. It is highly recommended that the use of this account be avoided.

Workflow status	RECORD STATE
New	ACTIVE
Set by the finding provider	
AWS account ID	Severity (original)
[REDACTED]	90 +
Severity (normalized)	Status
90 +	FAILED +

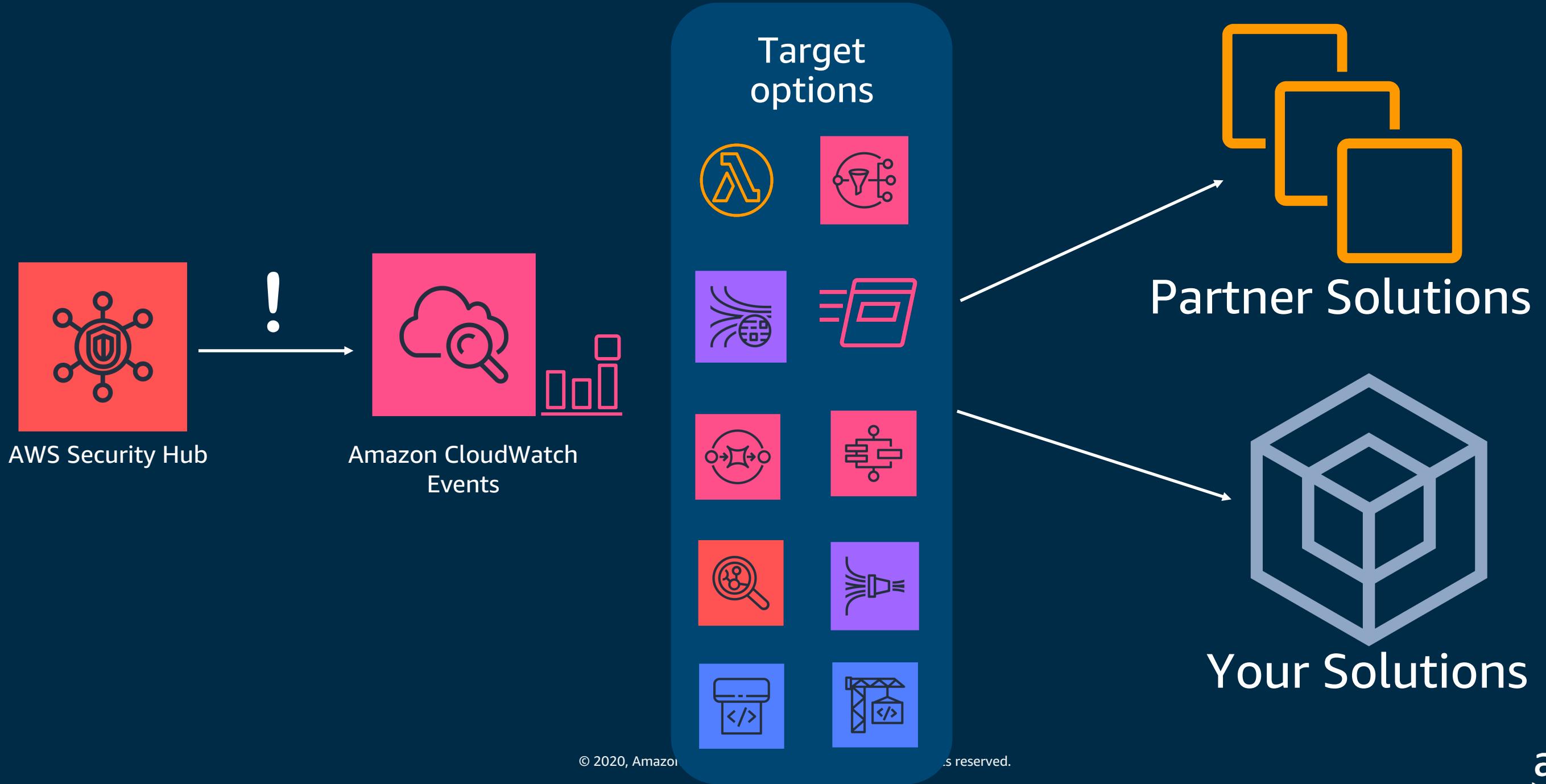
Insights



AWS Security Hub Information Flows



Taking action with Security Hub



Taking action on all findings

Every new Security Hub finding is sent to 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 i Schedule i

Build event pattern to match events by service

Service Name: Security Hub

Event Type: All Events

All Events

Security Hub Findings - Custom Action

Security Hub Findings - Imported

Security Hub Insight Results

AWS API Call via CloudTrail

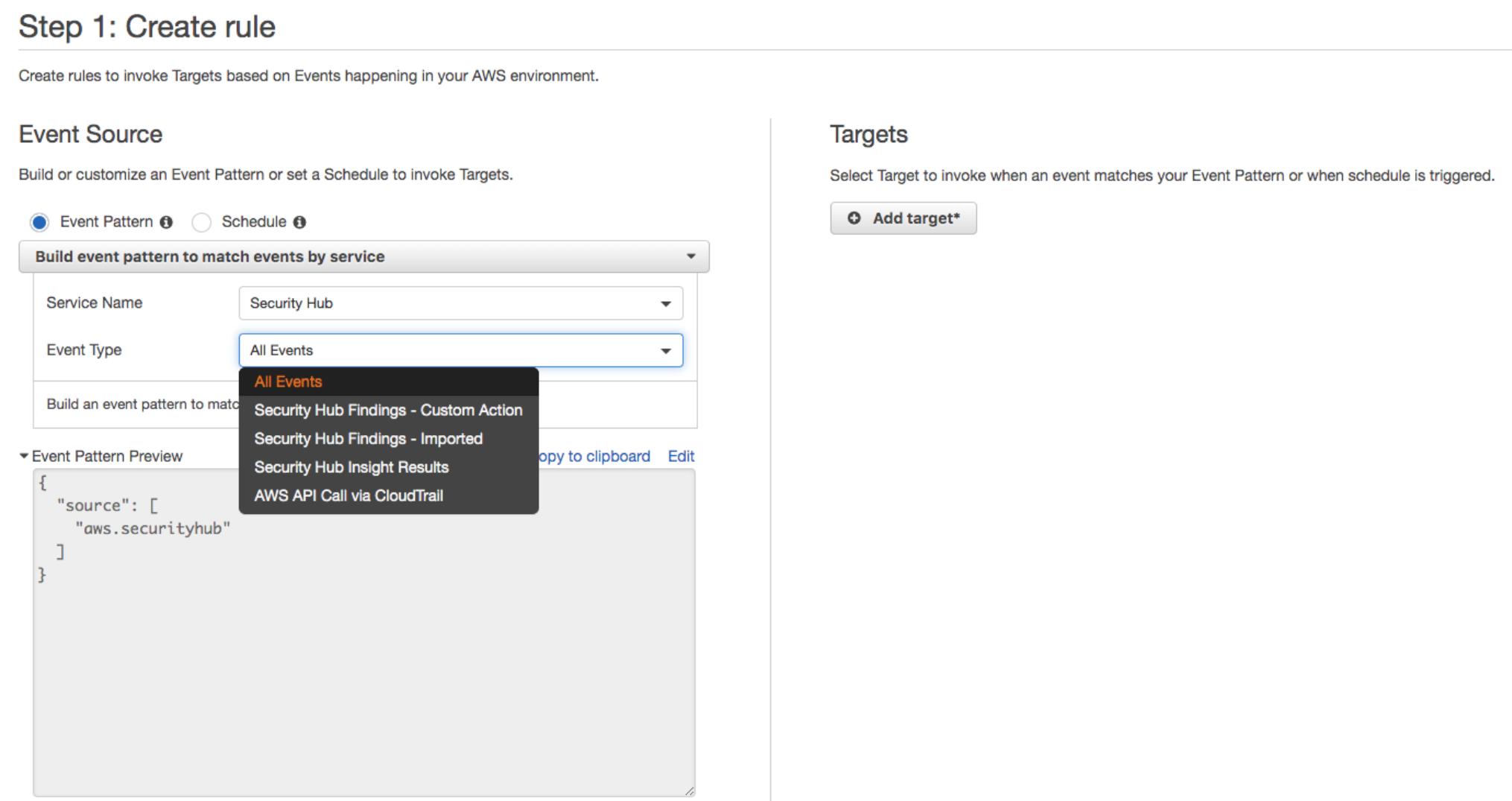
Event Pattern Preview:

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

Targets

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

Add target*



Event pattern examples

Filter by tags

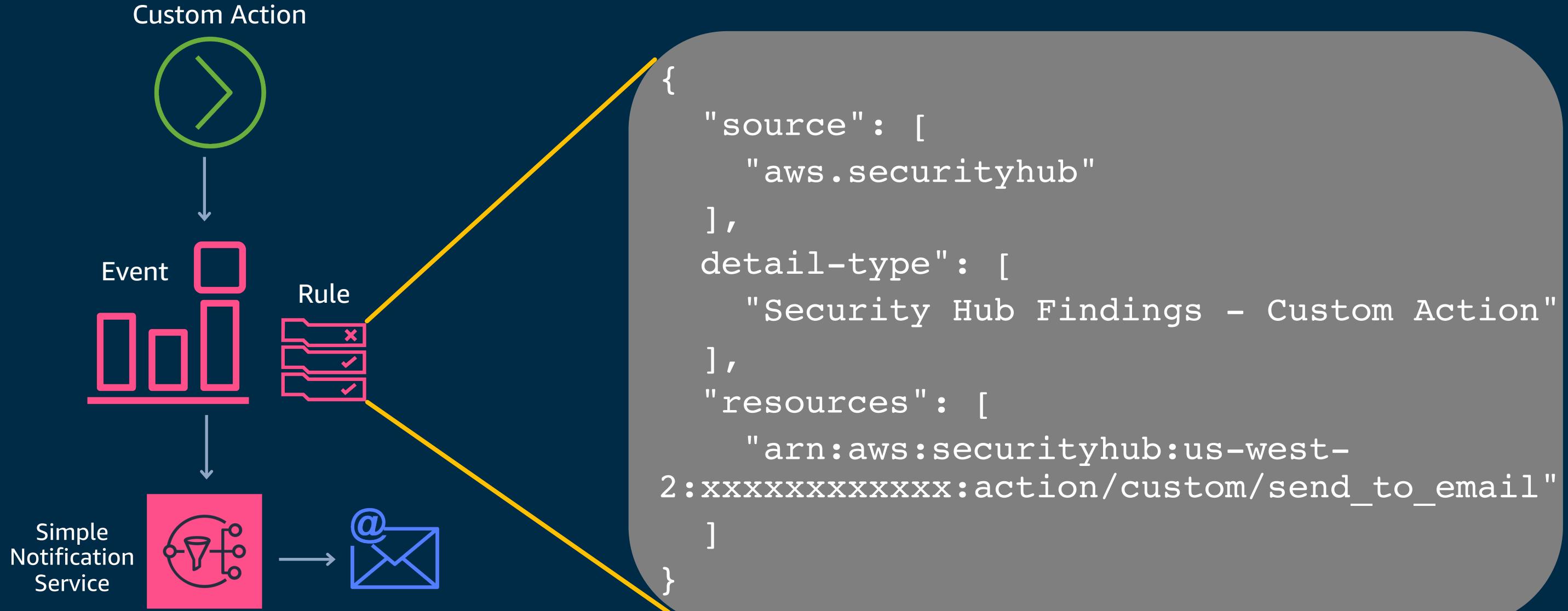
```
{  
  "source": [  
    "aws.securityhub"  
>],  
  "detail-type": [  
    "Security Hub Findings - Imported"  
>],  
  "detail": {  
    "findings": {  
      "Resources": {  
        "Tags": {  
          "Environment": [  
            "PCI"  
>]  
        }  
      }  
    }  
  }  
}
```

Event pattern examples

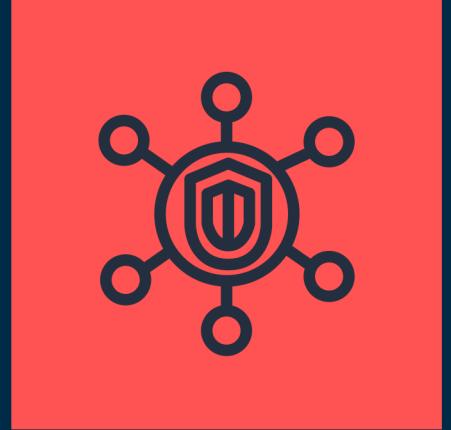
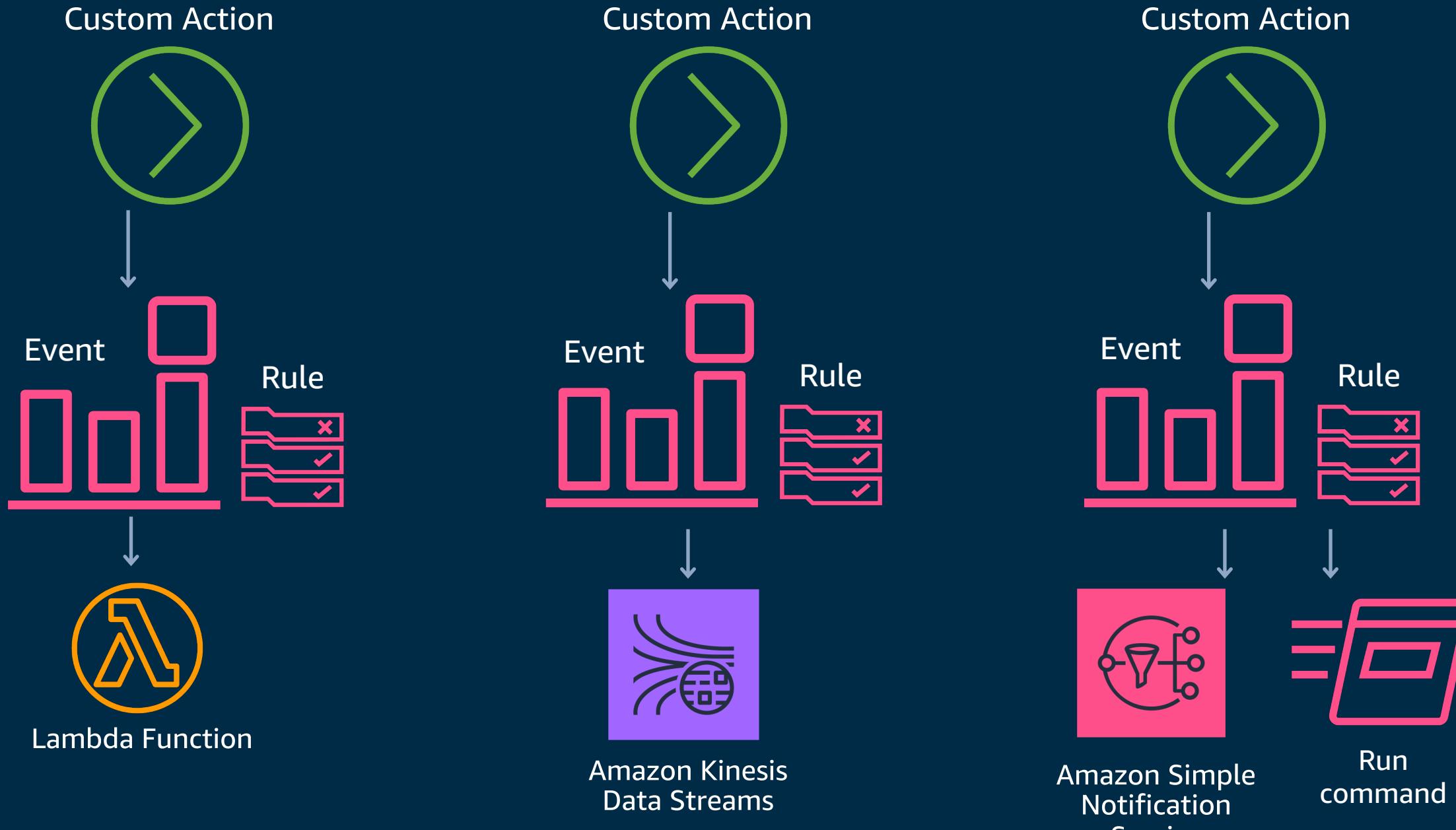
Filter by severity

```
{  
  "source": [  
    "aws.securityhub"  
>],  
  "detail-type": [  
    "Security Hub Findings - Imported"  
>],  
  "detail": {  
    "findings": {  
      "Severity": {  
        "Normalized": [  
          {  
            "numeric": [  
              ">=",  
              90  
>            ]  
          }  
        ]  
      }  
    }  
  }  
}
```

Custom actions in Security Hub



Custom actions in Security Hub



Workshop Details

High level view of the workshop

- ✓ Tour of Security Hub
- ✓ Create custom insights and custom findings
- ✓ Implement custom actions and remediation
- ✓ Implement finding enrichment and notification

Tour Security Hub

Guide on key features of Security Hub

Create custom insights and custom findings

Identify non-compliant instances via AWS Config Rules, create and visualize findings in Security Hub.

Implement custom actions and remediation

Custom lambda function to isolate an EC2 instance

Deploy remediation playbooks for CIS Benchmarks

Implement finding enrichment and notification

Post Security Hub findings into a Slack

Custom action to add EC2 Tags to finding notes

Have Fun Ask Questions

Workshop Guide

<https://github.com/aws-samples/aws-security-hub-workshop/blob/master/docs/index.md>