Hands-on with AWS Security Hub

Agenda

Security Hub Overview

Inbound Integrations

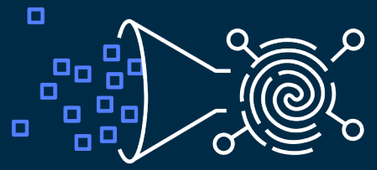
Outbound Integrations – Taking action

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.

f5

paloalto NETWORKS

imperva

Barracuda

Check Point SOFTWARE TECHNOLOGIES LTD.

Endpoint

CROWDSTRIKE

Symantec.

Vulnerability

tenable

Qualys. Continuous Security

RAPID7

Compliance

Check Point SOFTWARE TECHNOLOGIES LTD.

paloalto NETWORKS

Cloud Custodian

SOAR

DEMISTO

turbot

MSSP

ARMOR CLOUD SECURITY, UNCOMPROMISED.™

ALERT LOGIC

SIEM

IBM Security

sumologic

splunk>

Other

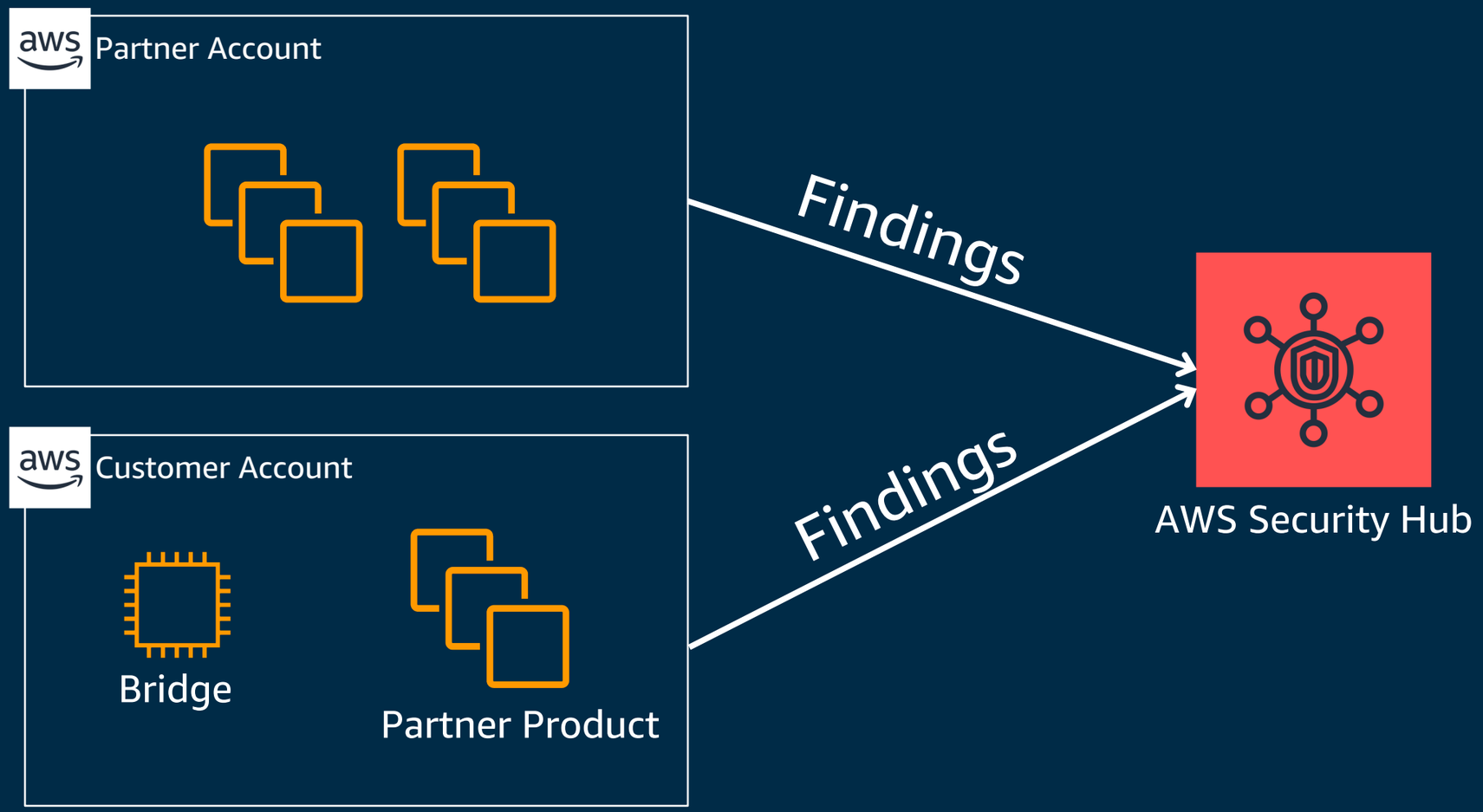
McAfee™ Together is power.

CYBERARK

Twistlock

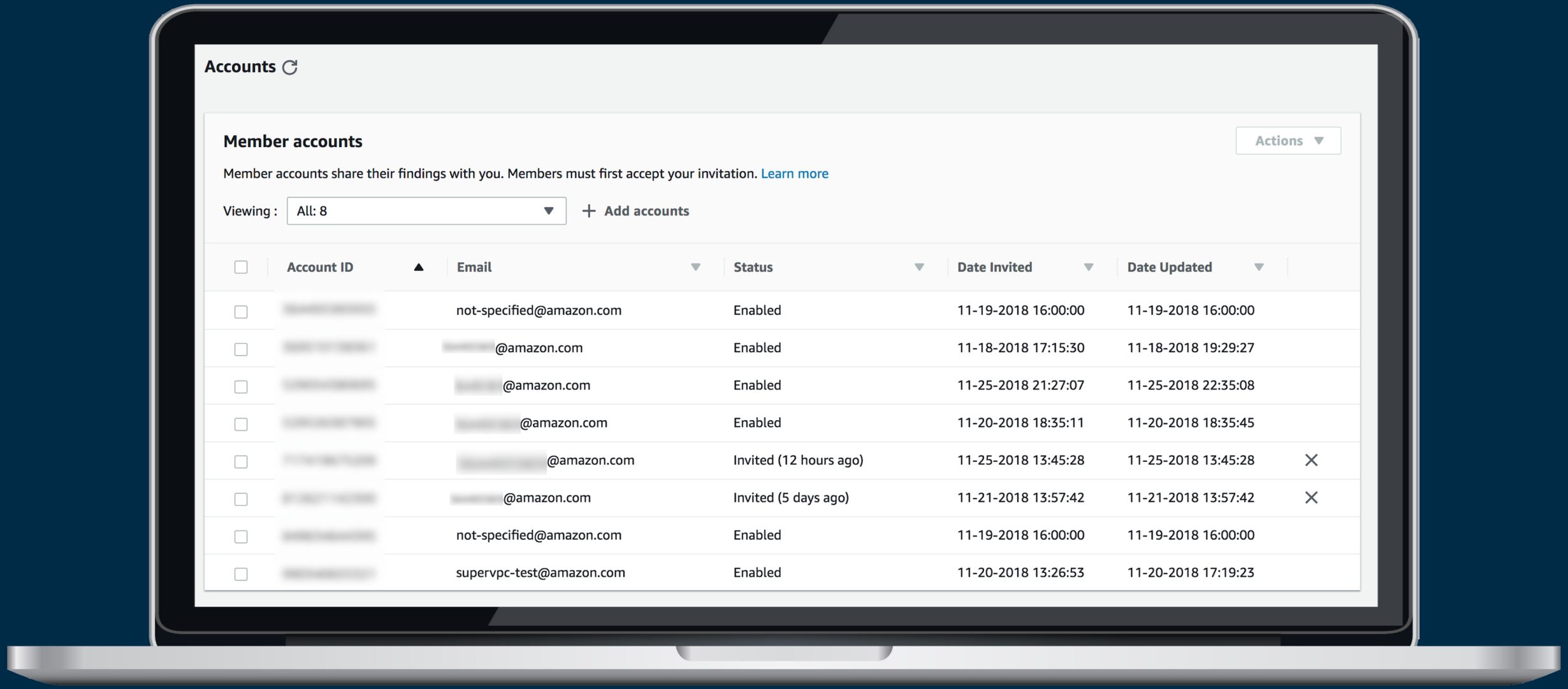
aws

Partner integrations – into Security Hub

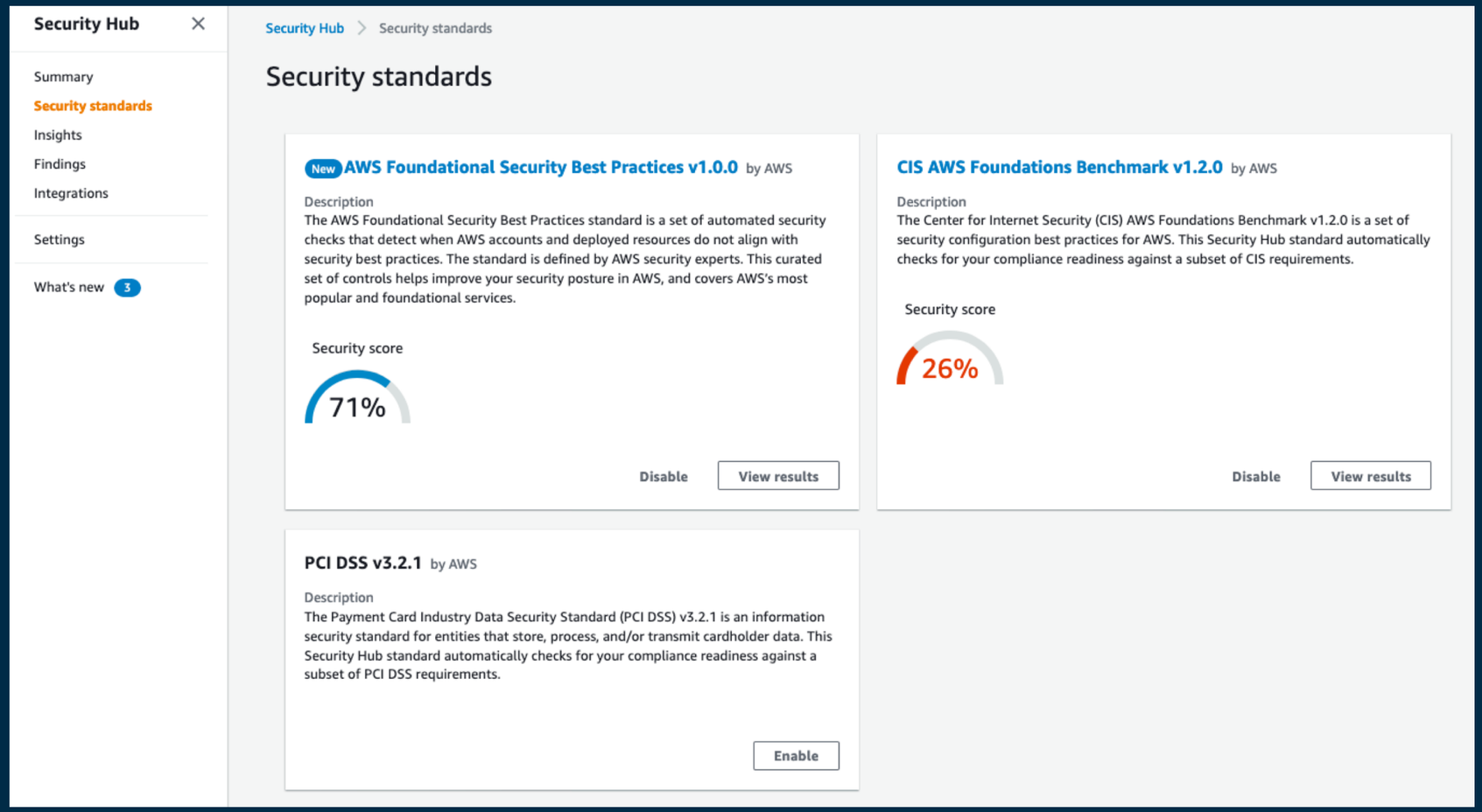


You can create your own findings

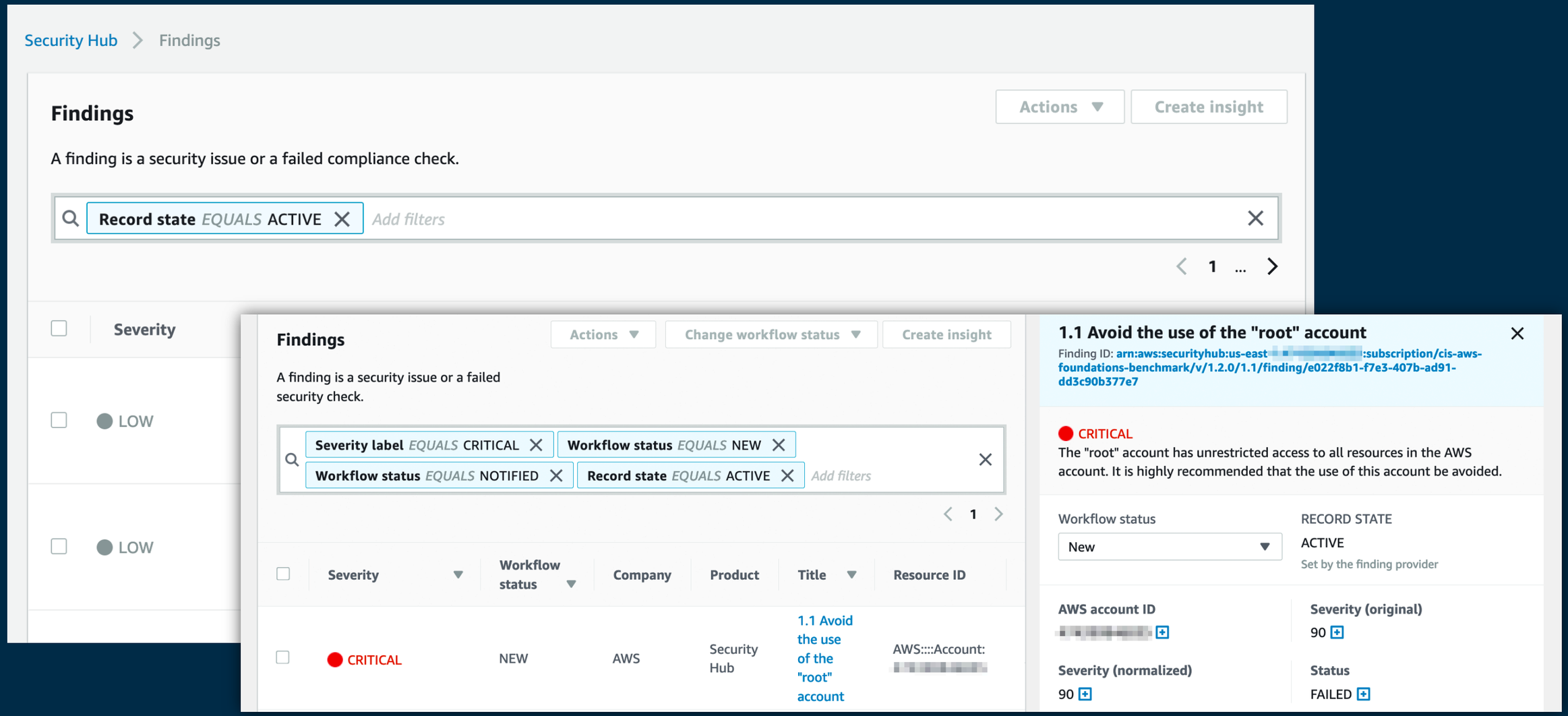
Setup and multi-account



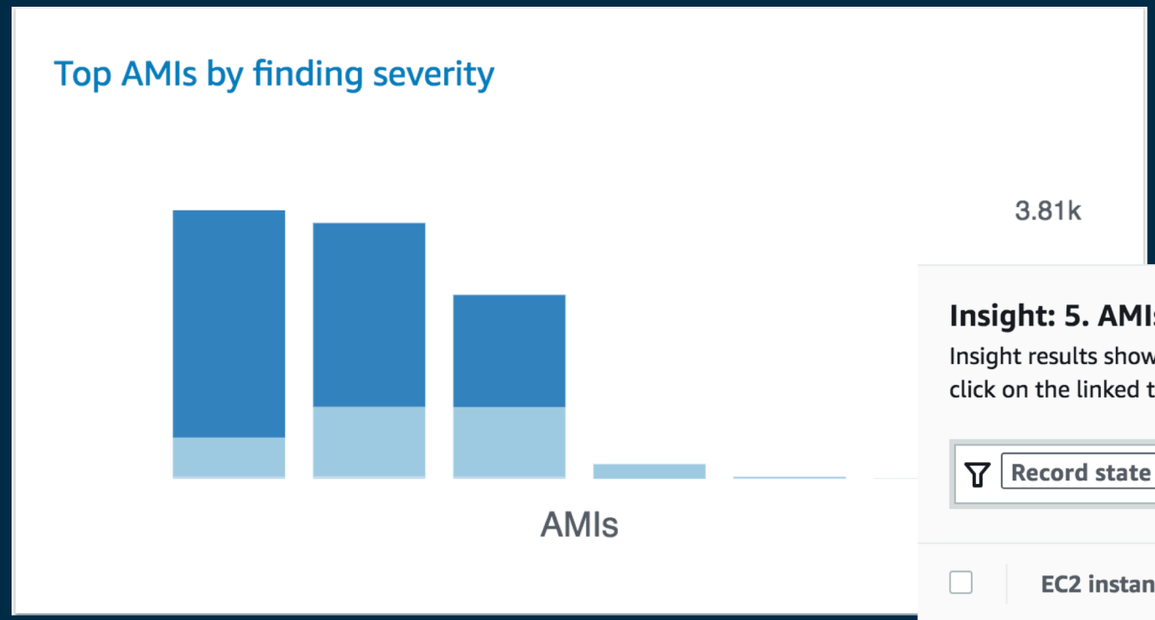
Security and Compliance checks



Findings



Insights



Insight: 5. AMIs that are generating the most findings

Actions ▼ | Create insight

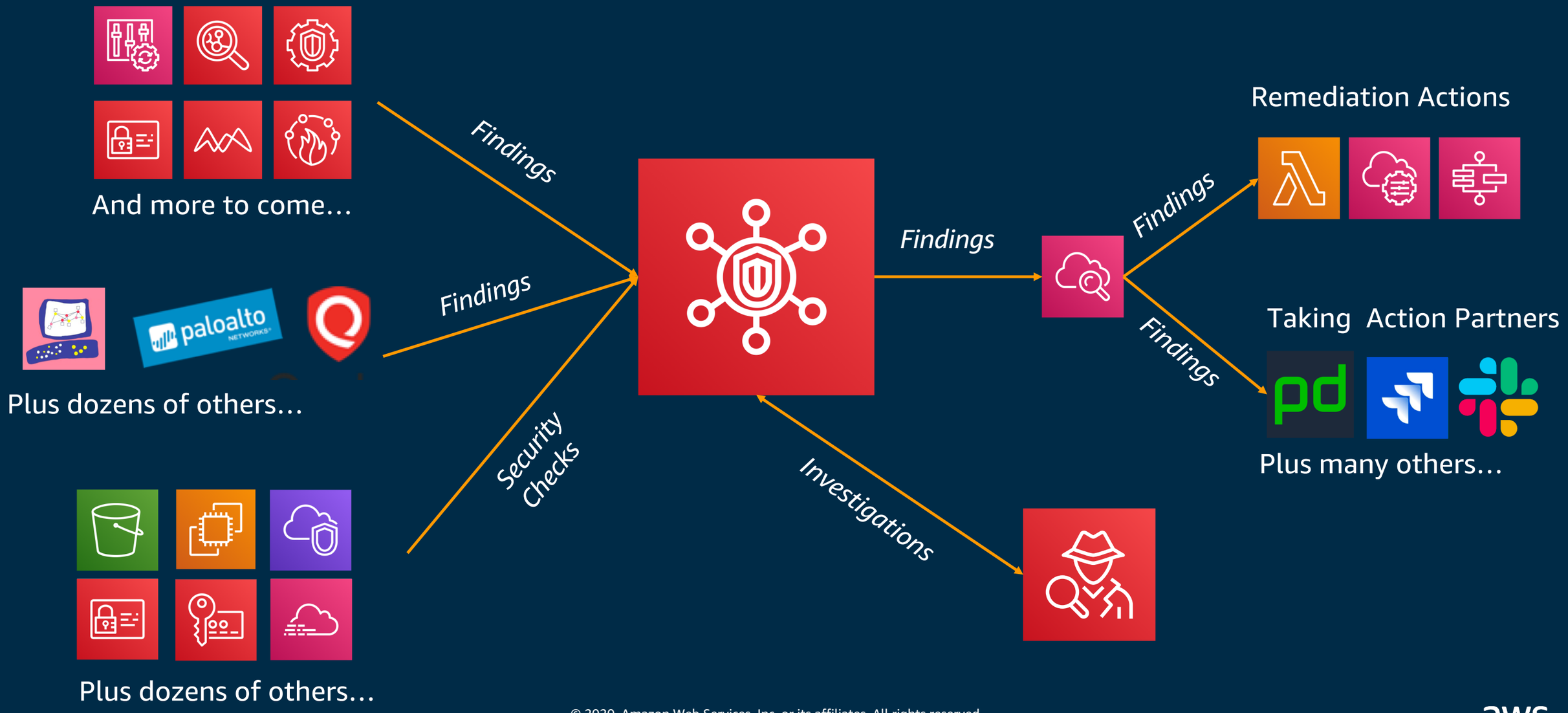
Insight results show an aggregated view of findings, typically by resource ID. To view the underlying findings of an insight result, click on the linked text below, or select a result(s) to take an action. You can also modify and save the insight definition

Record state *EQUALS* ACTIVE ⊗ | Group By: ResourceAwsEc2InstanceImageId ⊗ | *Add filter* ✕

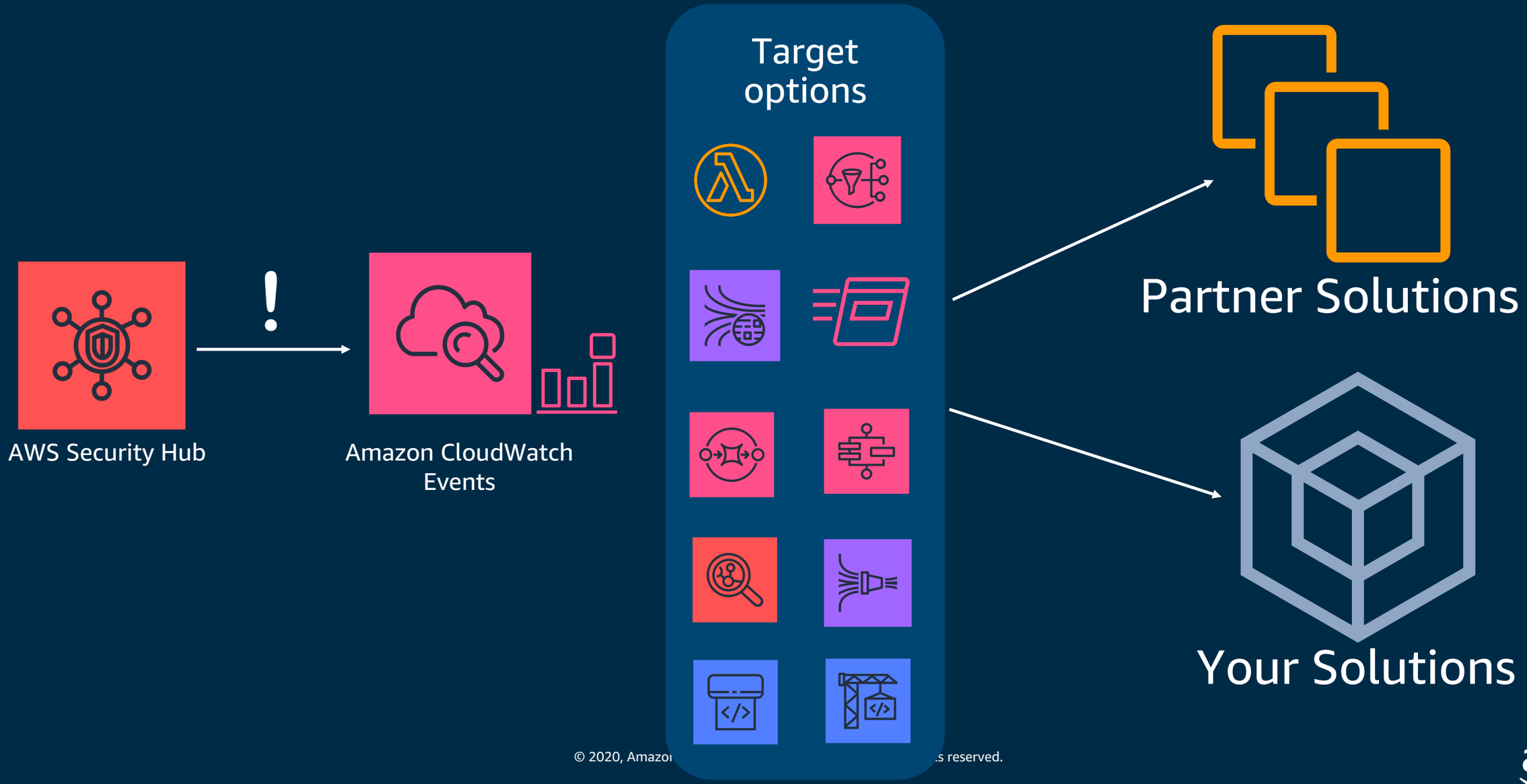
EC2 instance image ID	Count
ami-f2d3638a	4051
ami-d1c5d1e1	3729
ami-5d967725	2640
ami-f6f16b9f	753
ami-2a8f2f43	502
ami-31814f58	502

aws

AWS Security Hub Information Flows

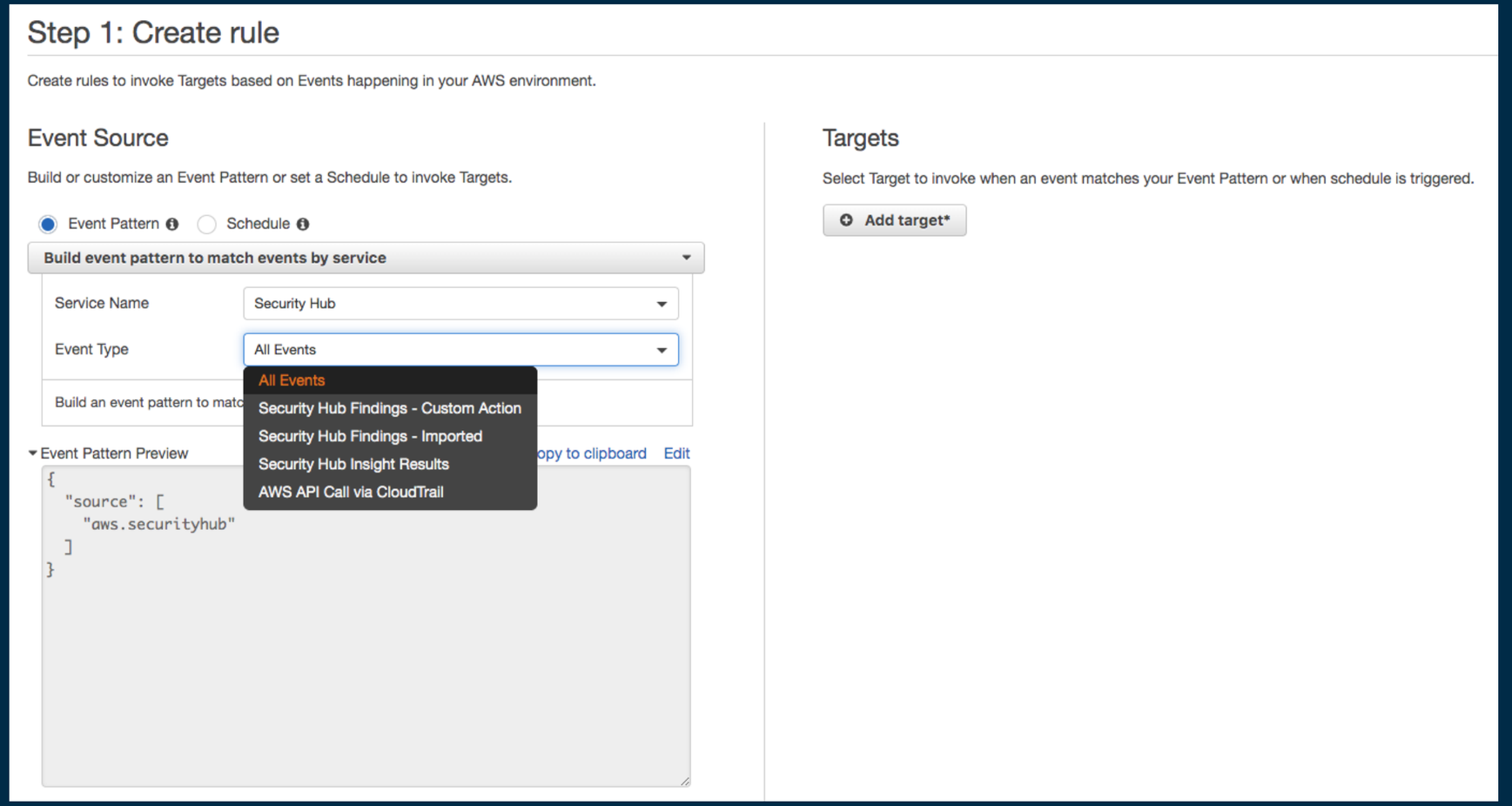


Taking action with Security Hub



Taking action on all findings

Every new Security Hub finding is sent to CloudWatch Events



Event pattern examples

Filter by tags

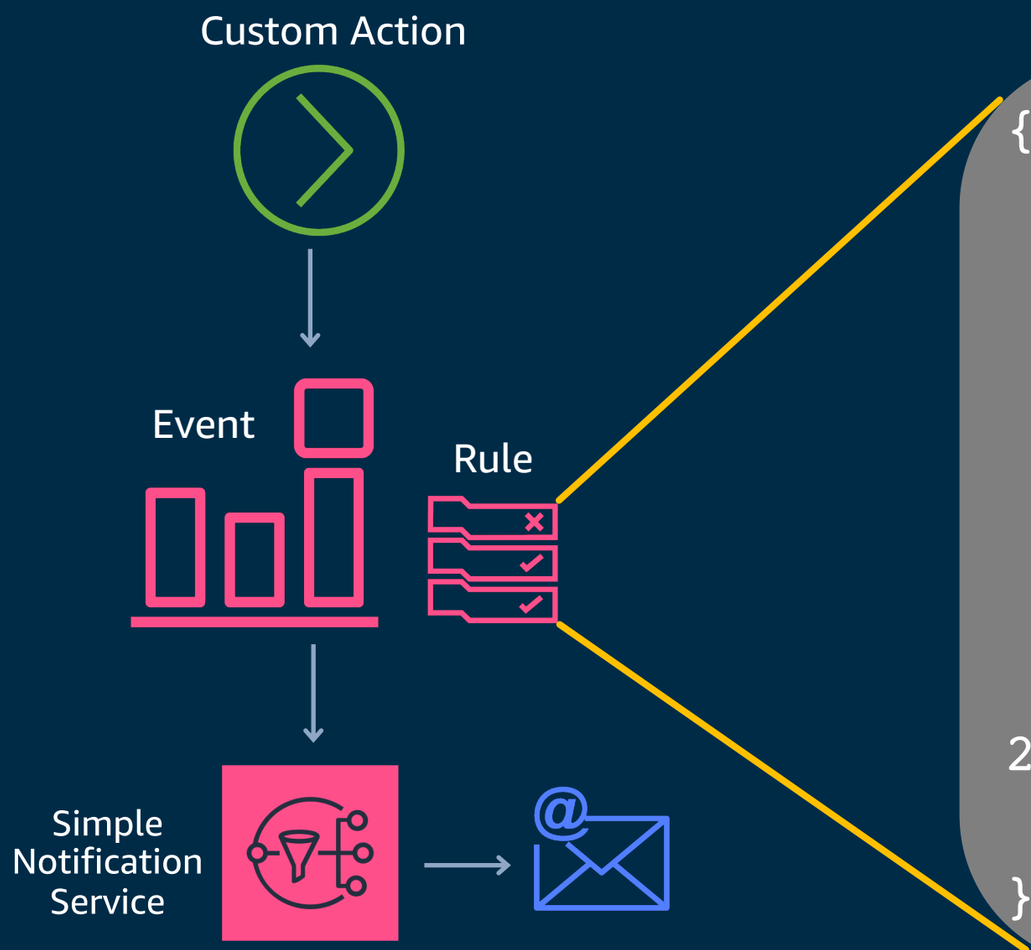
```
{
  “source”: [
    “aws.securityhub”
  ],
  “detail-type”: [
    “Security Hub Findings - Imported”
  ],
  “detail”: {
    “findings”: {
      “Resources”: {
        “Tags”: {
          “Environment”: [
            “PCI”
          ]
        }
      }
    }
  }
}
```

Event pattern examples

Filter by severity

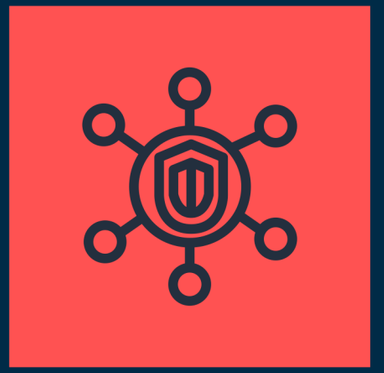
```
{
  “source”: [
    “aws.securityhub”
  ],
  “detail-type”: [
    “Security Hub Findings - Imported”
  ],
  “detail”: {
    “findings”: {
      “Severity”: {
        “Normalized”: [
        {
            "numeric": [
              ">=",
              90
            ]
        }
      ]
    }}}}
```

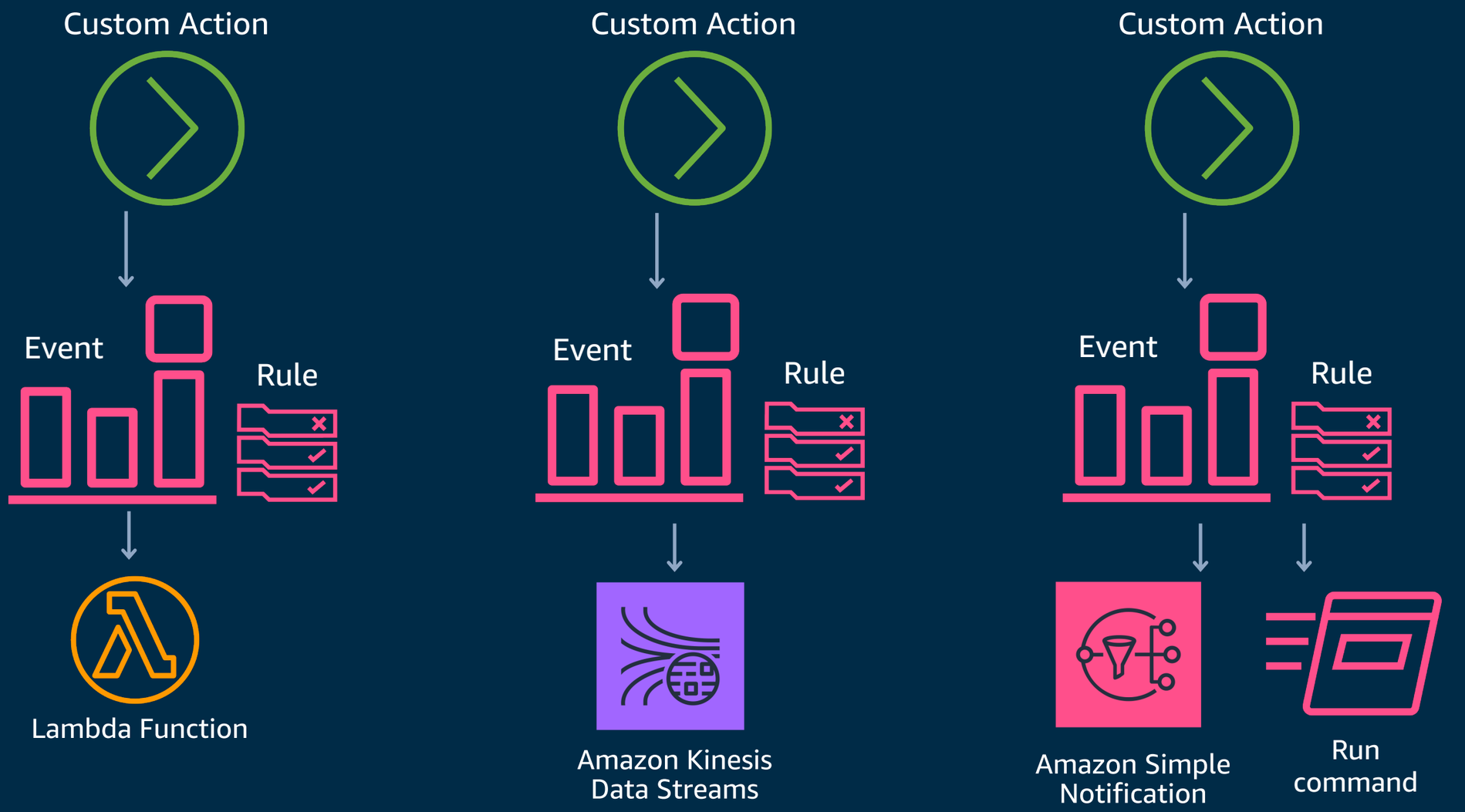
Custom actions in Security Hub




```
{
  "source": [
    "aws.securityhub"
  ],
  detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [
    "arn:aws:securityhub:us-west-
2:xxxxxxxxxxxx:action/custom/send_to_email"
  ]
}
```

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