AWS Security Hub

Partner Program

Agenda

Security Hub Partner Program Introduction

Security Hub Overview

Security Hub Demo

Next Steps

aws

Summary

- AWS Security Hub is AWS's security and compliance center
    - It aggregates and prioritizes alerts from AWS and partner products
    - It conducts automated compliance checks

- Partnerships are critical to Security Hub's success.
    - To date, we have ~30 product integrations with partners.
    - We are focused on highlighting partner capabilities
    - Partnering is focused on lightweight technical integrations

aws

Partner Value Proposition

1. **Customer satisfaction.** The number one reason to integrate with Security Hub is because you have customer requests to do so. Security Hub is the security and compliance center for AWS customers and is designed as the first stop where AWS-focused security and compliance professionals will go each day to understand their security and compliance state. Listen to your customers. They will tell you if they want to see your findings in Security Hub.

2. **Discovery opportunities.** We promote partners with certified integrations inside the Security Hub console, including links to their Marketplace listings. This is a great way for customers to discover new security products.

3. **Marketing opportunities.** Vendors with approved integrations can participate in webinars, press releases, create slick sheets, and demonstrate their integrations to AWS customers.

aws

Types of Partners

1. Findings providers
    - Send findings from within the customer accounts
    - Send findings from your AWS account
2. Findings consumers
    - Consume via GetFindings API (using cross-account roles)
    - Consume via CloudWatch Events (as a target for custom actions)
3. Partners that do both 1 and 2
4. Consulting partners that assist customers with deploying and customizing Security Hub

aws

Partner integrations

Firewalls


Endpoint

Vulnerability

Compliance

SOAR

MSSP

SIEM

Other

aws

What about consulting partners?

MSSP partners should must demonstrate how Security Hub would plug into their customer workflows (i.e., define the use case for your customers), as part of their technical integration with Security Hub.

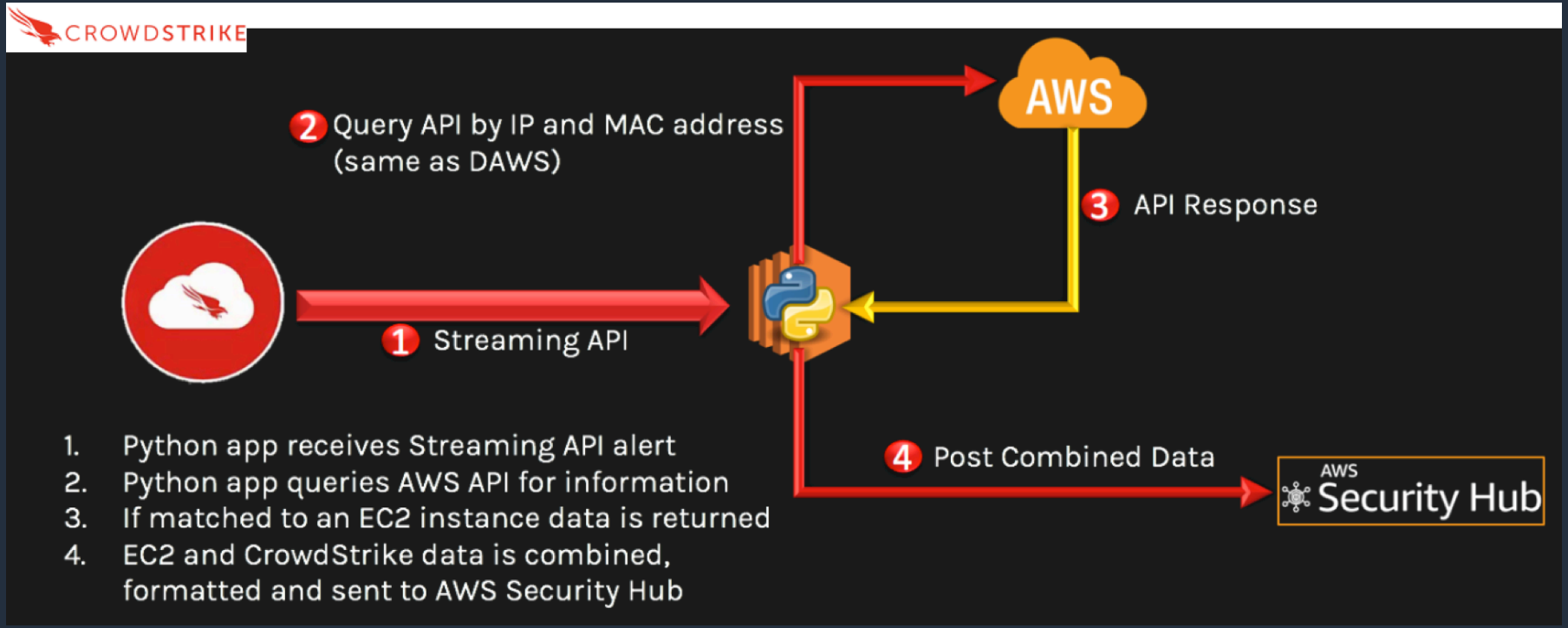
Non-MSSP consulting partners can also become Security Hub partners. They should submit two case studies on how they helped a specific customer do the following:

1. Setup SecHub with IAM permissions needed by the customer
2. Assist in connecting already integrated ISV solutions to SecHub using the configuration instructions on the partner page in the console.
3. Assist customers in custom product integrations
4. Build custom insights relevant to customer needs/datasets
5. Build custom actions

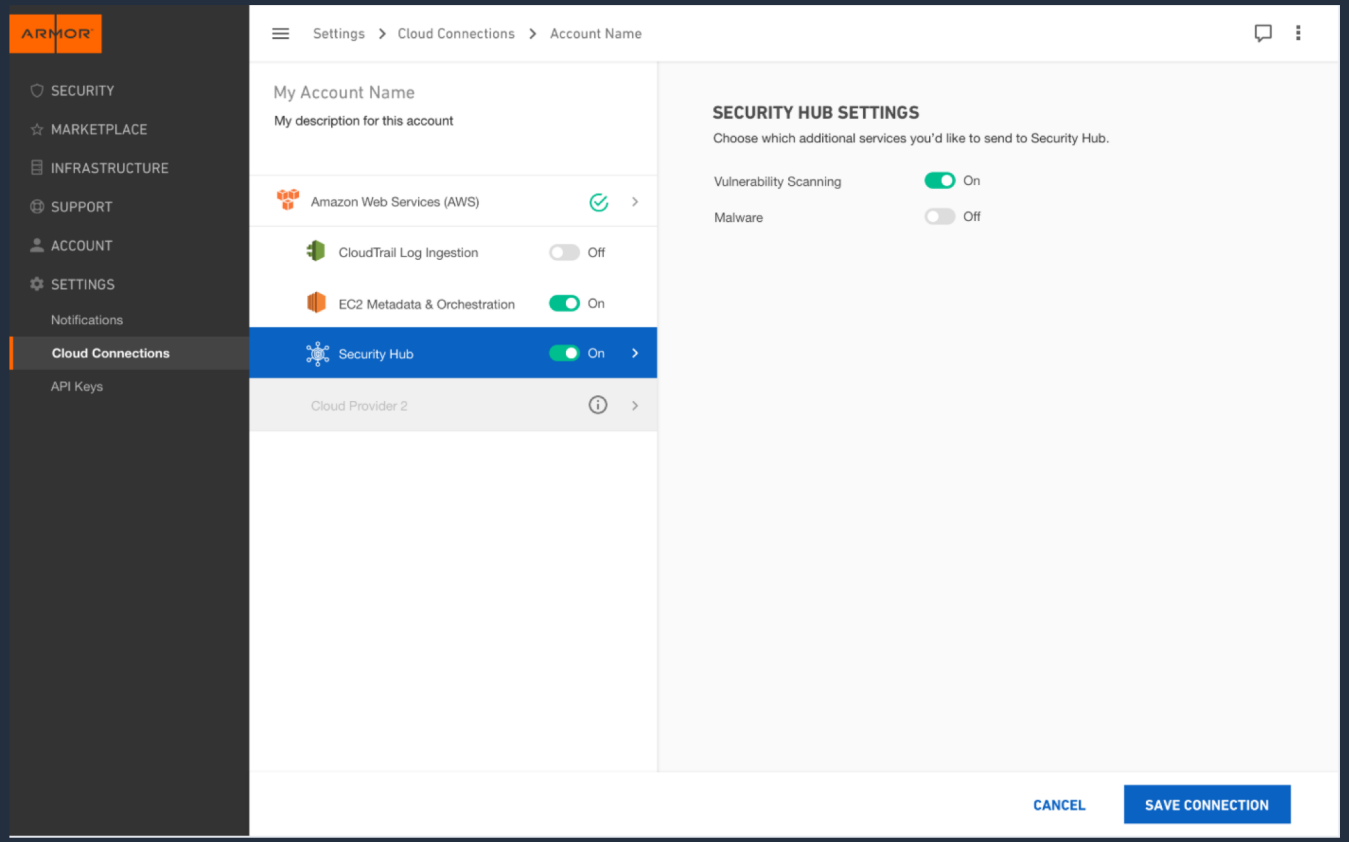
Case studies should be publicly shareable and must address at least 3 of the 5 bullets above.

aws

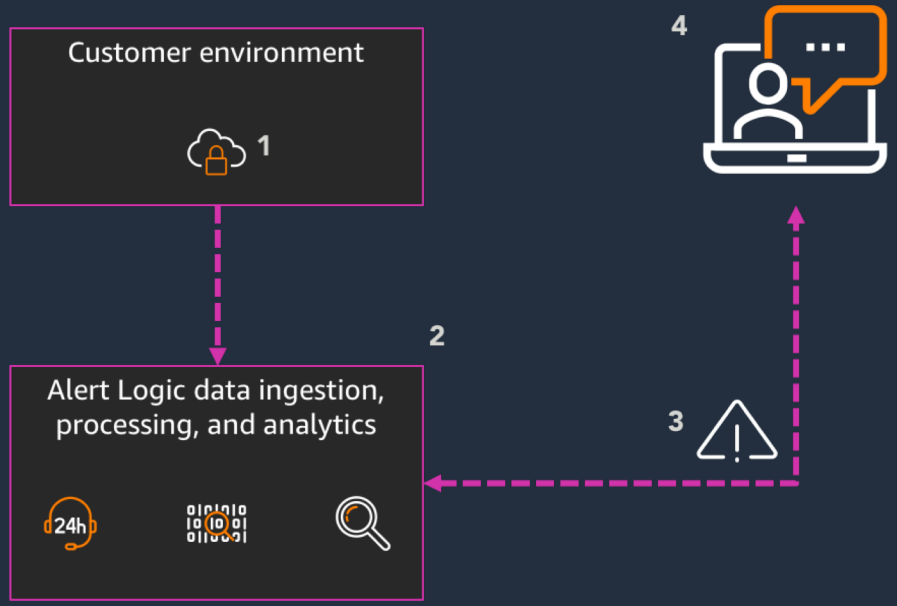
Partner integration examples — CrowdStrike



Partner integration examples — Armor

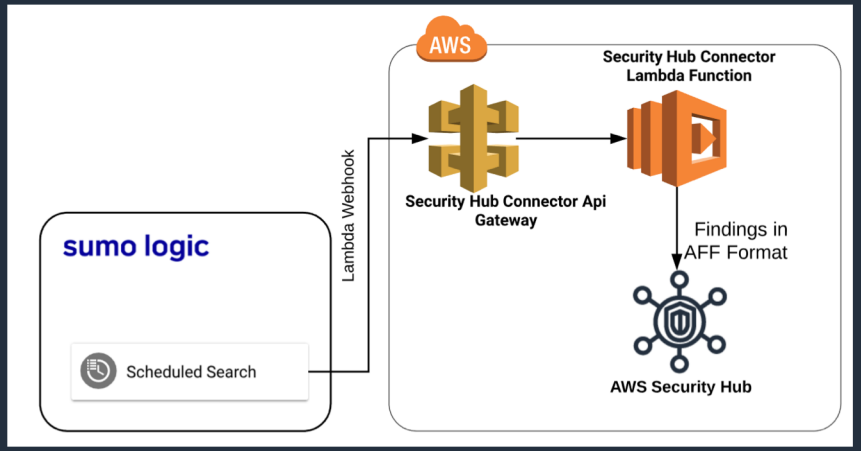


Partner integration examples — Alert Logic



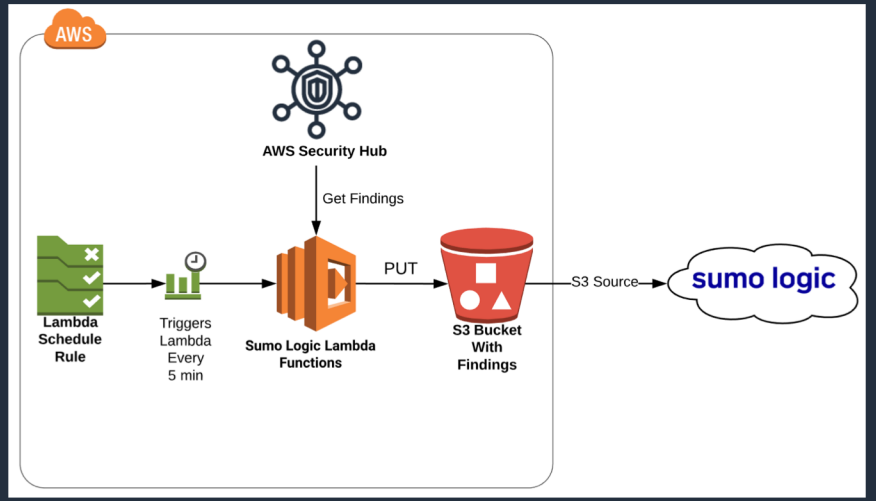
1. Inspected data is transported to Alert Logic's data ingestion, processing, and analytics platform
2. Alert Logic's **threat detection and response** capability analyzes the data and identifies **incidents**
3. An internal service (dedicated to AWS Security Hub) assesses the **incident** for potential posting to AWS Security Hub
4. The **incident** is then posted to the respective customer's AWS Security Hub console as a **finding**

Partner integration examples — Sumo Logic

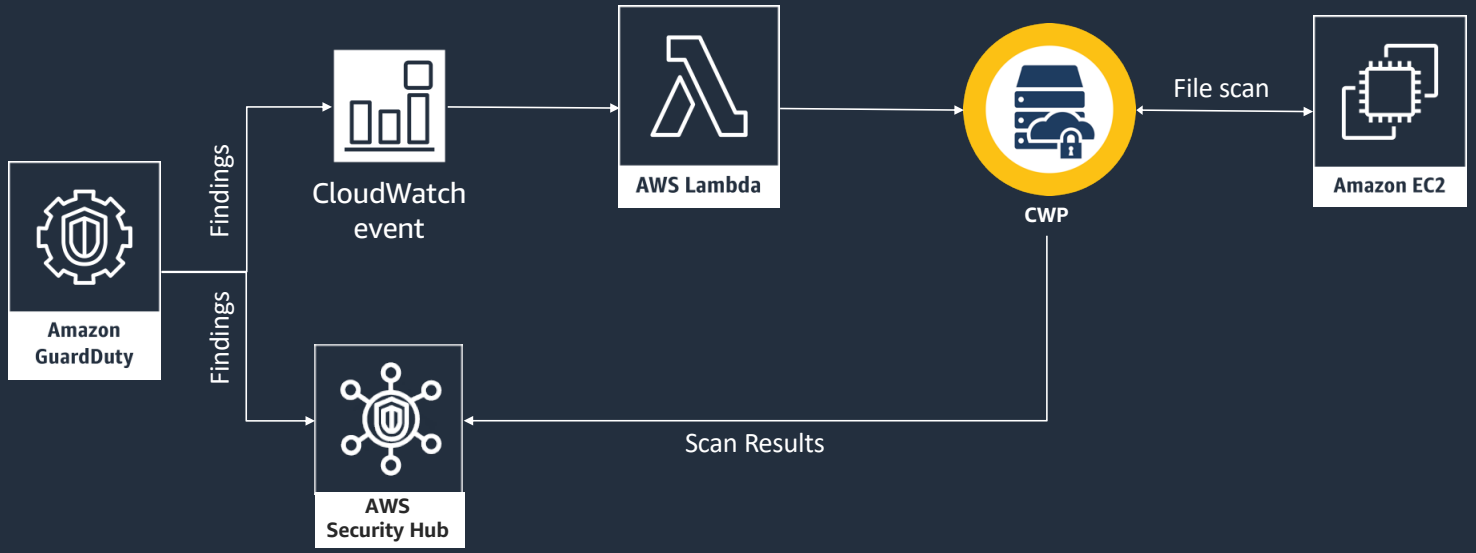


Sumo Logic sends findings to SecHub

Sumo Logic gets findings from SecHub



Partner integration examples — Symantec



Permissions

- IAM Policies
  - IAM policies must be configured for the IAM user/role calling BatchImportFindings (and other API calls)
  - You can start with allowing all actions on all resources and then restricting down

- Resource Policies
  - Security Hub also uses resource policies to validate that a customer authorizes a partner to send (or receive) findings to its Security Hub account
  - These resources polices can be put in place via the UI or API; they can be put in place by the customer or a partner working on behalf of the customer using cross-account roles.

Process

1. Submit your partner manifest information.
2. Receive Product ARNs to use with Security Hub.
3. Map your findings to ASFF.
4. Define your architecture for sending/receiving/pulling findings to/from Security Hub.
5. Create a deployment framework for customers (e.g., CloudFormation scripts).
6. Document your setup/configuration instructions for customers.
7. Define any default insights (aka correlation rules) for your product.
8. Demo your integration to the Security Hub team.
9. Submit marketing information for approval (website language, press release, slick sheet)

Typically, this process takes 4-6 weeks end-to-end

aws

Agenda

Security Hub Partner Program Introduction

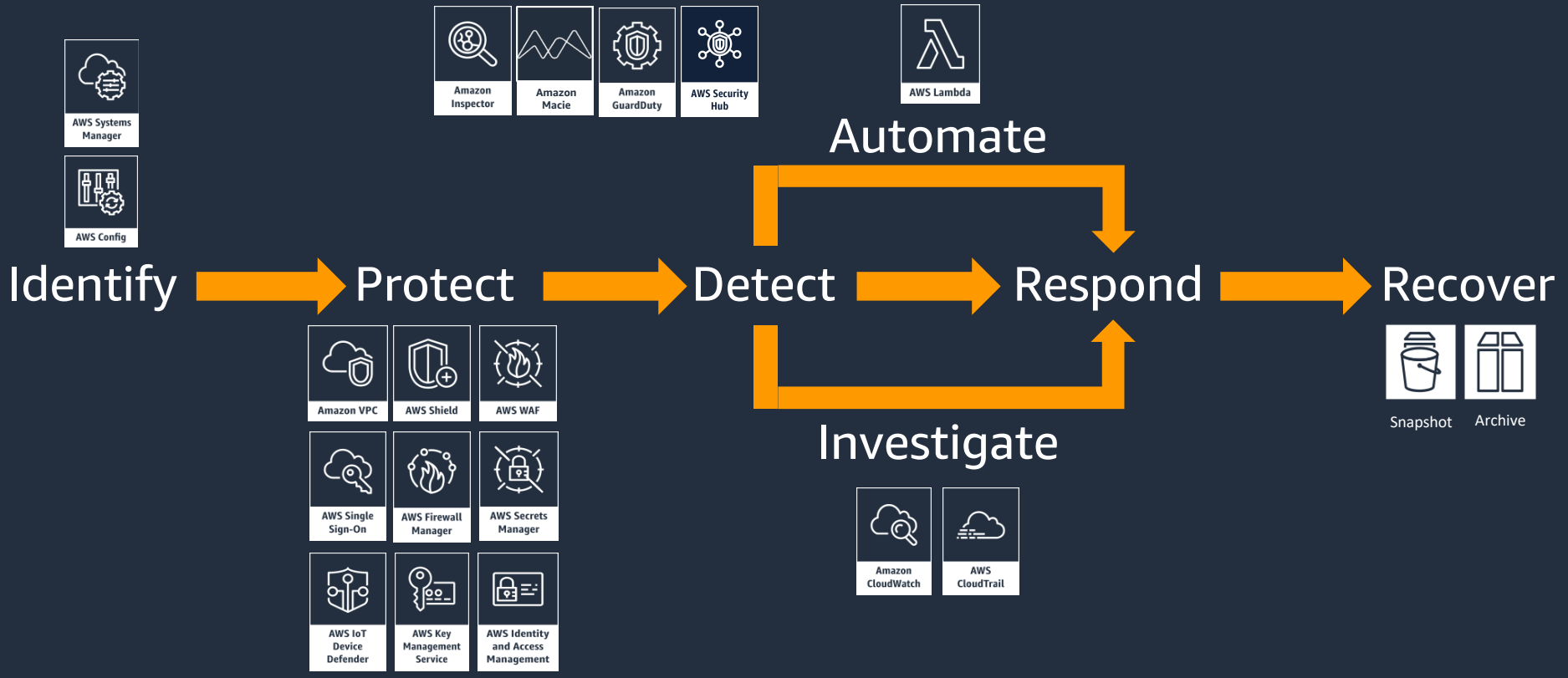
Security Hub Overview

Security Hub Demo

Next Steps

aws

AWS security overview



Problem statement

Compliance

1. Ensure that your AWS infrastructure meets compliance requirements

Multiple formats

2. Dozens of security tools with different data formats

Prioritization

3. Large volume of alerts and the need to prioritize

Visibility

4. Lack of a single pane of glass across security and compliance tools

aws

AWS Security Hub overview

Rollout plans and pricing

AWS Security Hub is available today as a public preview service

- Available at no additional cost except for AWS Config costs for new AWS Config users
- Open to everyone
- Get started in a few clicks
- Goal is to iterate on latest features with customers before releasing as generally available (GA)

Full API/CLI/SDK support

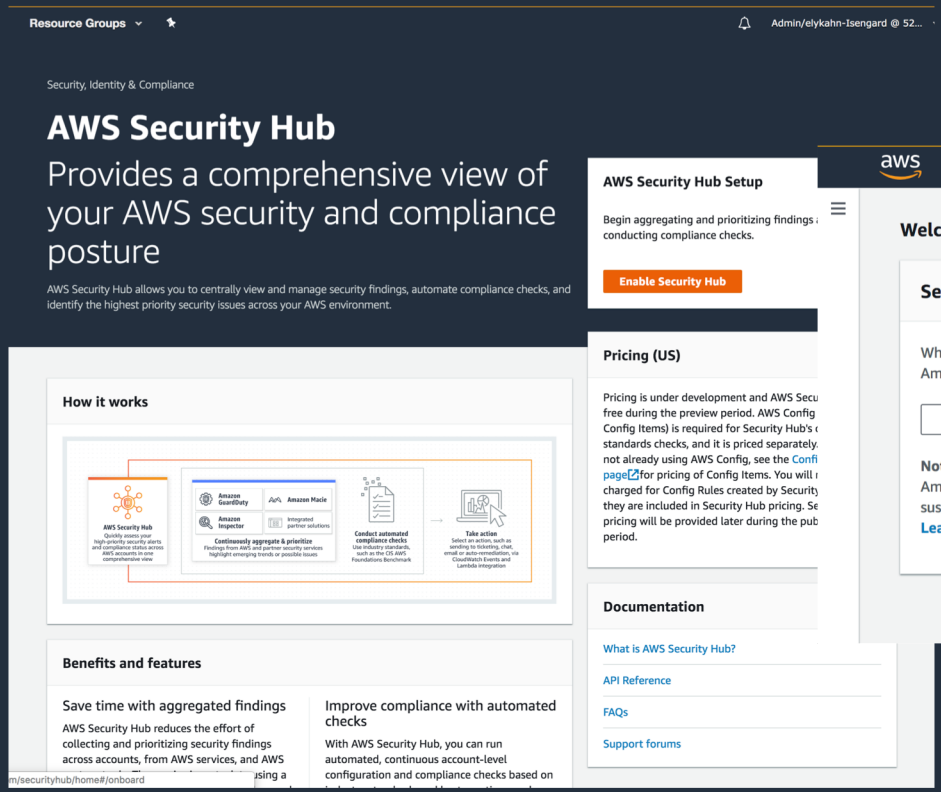
- C++, Go, Java, JS, .Net, PHP, Python, Ruby

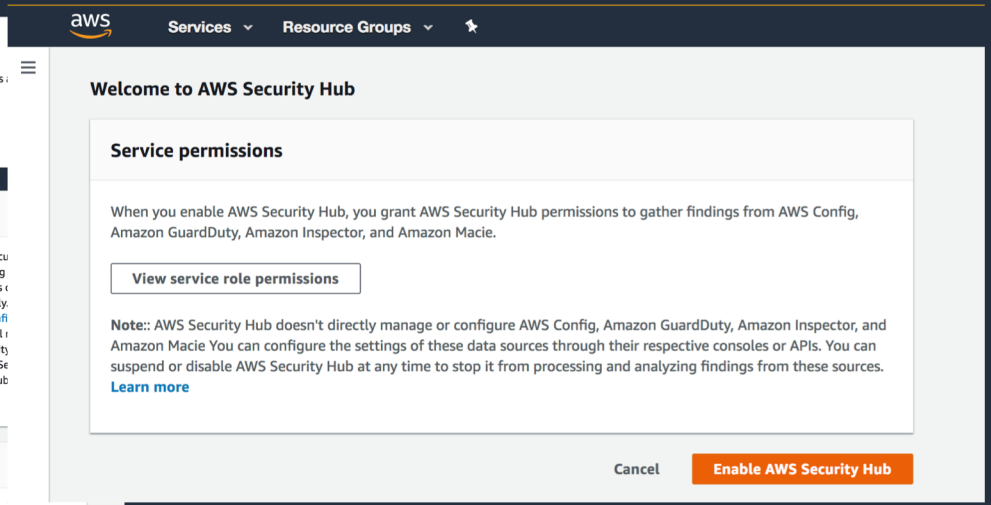
Supported Regions (15)

- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- EU (Frankfurt
- EU (Ireland)
- EU (London)
- EU (Paris)
- South America (Sao Paulo)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

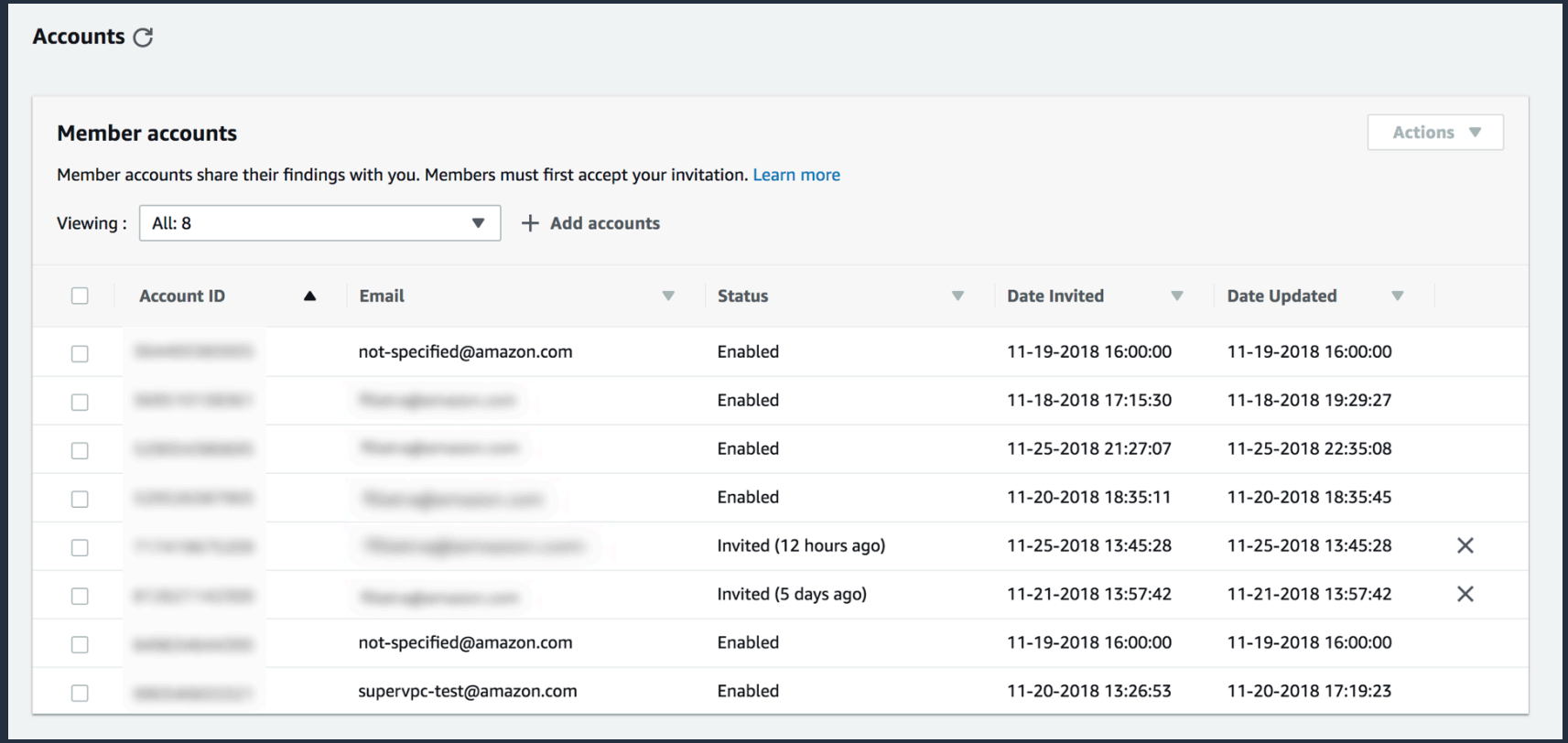
aws

A few clicks to enable Security Hub





Simple multi-account setup

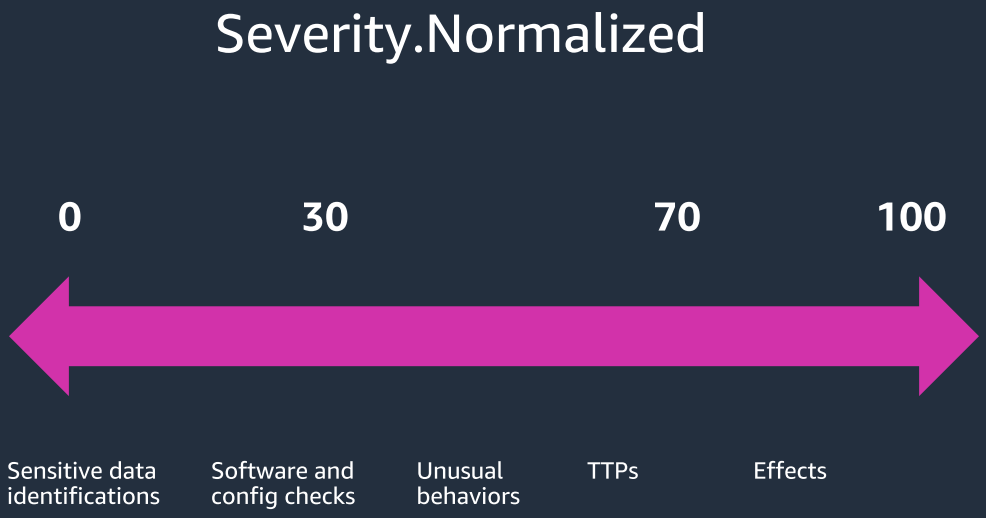


AWS Security Finding Format

~100 JSON-formatted fields

Finding Types

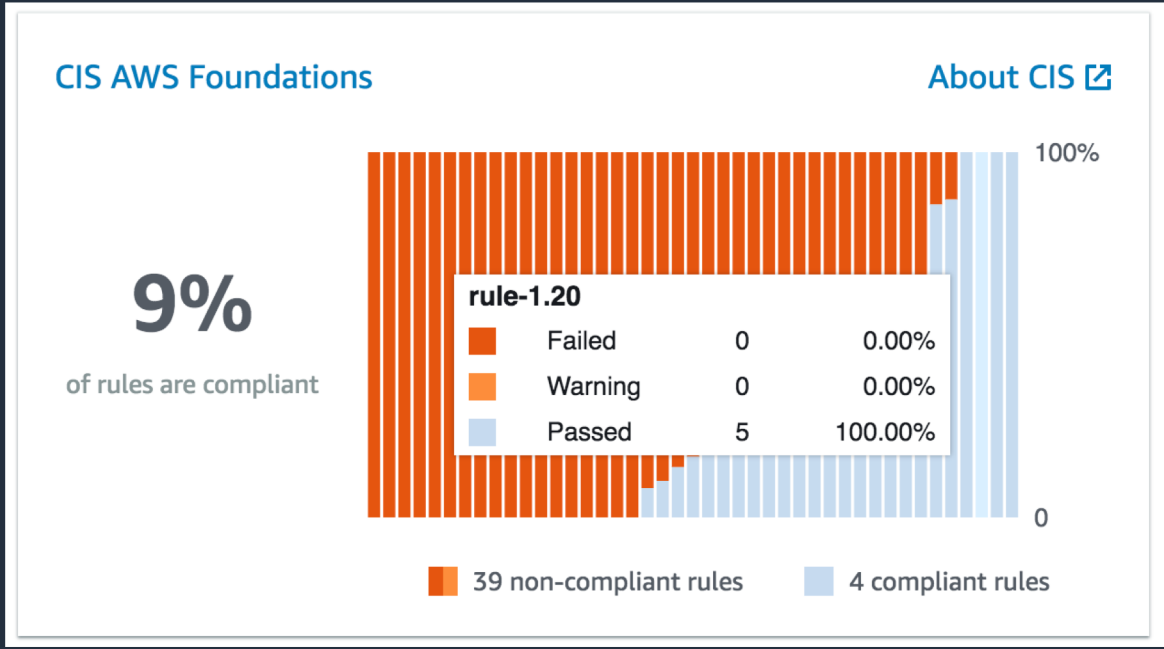
- Sensitive Data Identifications
- Software and Configuration Checks
- Unusual Behaviors
- Tactics, Techniques, and Procedures (TTPs)
- Effects



Automated compliance checks

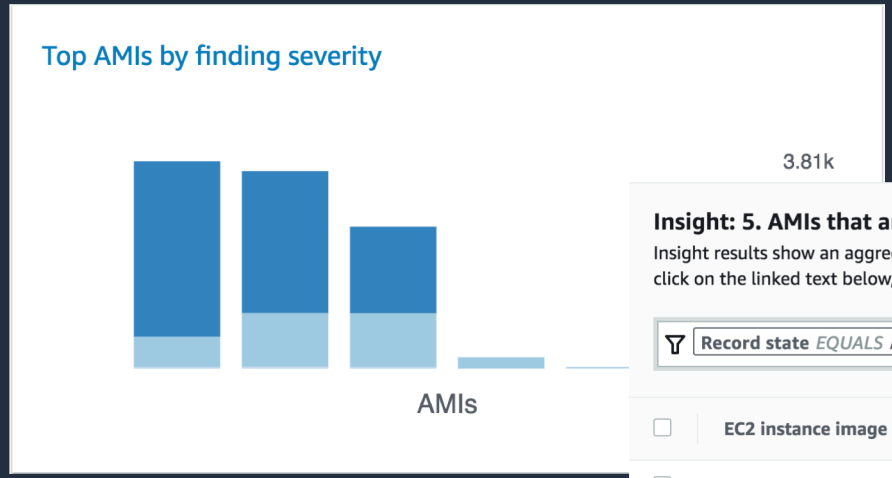
CIS Center for Internet Security®

43 fully automated, nearly continuous checks



aws

Insights help identify resources that require attention



Insight: 5. AMIs that are generating the most findings

Actions ▼ | Create insight

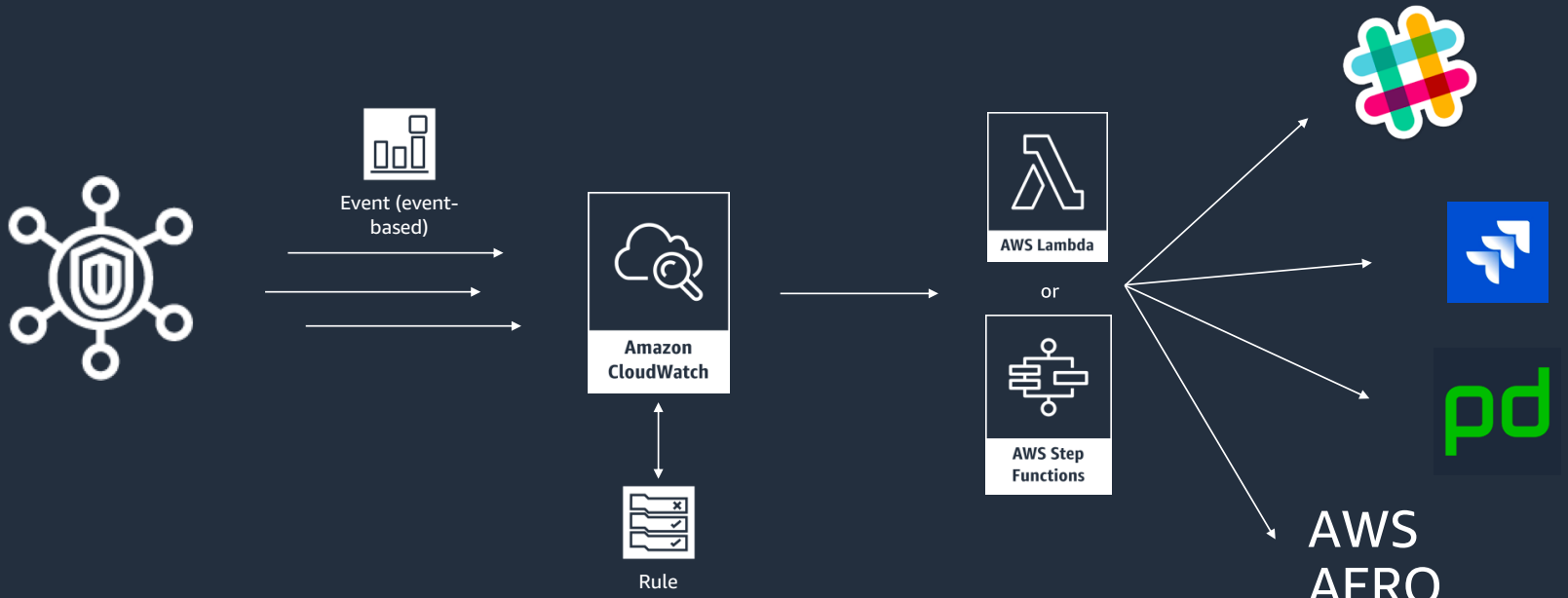
Insight results show an aggregated view of findings, typically by resource ID. To view the underlying findings of an insight result, click on the linked text below, or select a result(s) to take an action. You can also modify and save the insight definition

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

Customizable response and remediation actions



1. AWS Security Hub user selects findings in the console and takes a custom action on them

2. Findings are sent to CloudWatch decorated with a custom action ID

3. The custom action ID is used to match up with a CloudWatch Event rule

4. The rule defines a target – typically a Lambda or Step Function

5. The target could be things like a chat, ticketing, incident management or remediation system

Key takeaways

- Understand and manage your overall AWS security and compliance posture
- Evaluate your compliance against regulatory and best practice frameworks
- Collect and process security findings from multiple accounts within a region
- Identify and prioritize the most important issues by grouping and correlating security findings with Insights

aws

Agenda

Security Hub Partner Program Introduction

Security Hub Overview

Security Hub Demo

Next Steps

aws

Demo

Agenda

Security Hub Partner Program Introduction

Security Hub Overview

Security Hub Demo

Next Steps

aws

Next steps

1. Submit an email alias we can use for your team
2. Submit specific emails that you would like to be added to Slack channel and weekly technical office hours with the product team
3. Submit your partner manifest
4. Begin mapping your findings to ASFF and design your architecture

aws

Points of contact

[PDM / Partner SA contact]

Product team contact: securityhub-partners@amazon.com

Learning more

Try the preview: https://console.aws.amazon.com/securityhub/

Learn more: https://aws.amazon.com/security-hub/

Documentation:

https://docs.aws.amazon.com/securityhub/index.html#lang/en_us