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 security checks

- Partnerships are critical to Security Hub's success.
    - To date, we have ~50 product integrations with partners.
    - We are focused on highlighting partner capabilities
    - Partnering involves building a lightweight technical integration (4-8 weeks of developer work)

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.** We are happy to participate **in vendors' marketing efforts, such as** webinars, press releases, use cases, and demos. Also, you can submit a blog to the AWS Partner Network Blog.

aws

Types of Partners

1. Findings providers
    - Send findings from within the customer accounts
    - Send findings from your AWS account
2. Findings consumers
    - Consume all findings via CloudWatch Events
    - Consume specific findings selected by the customer for action 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

What about consulting partners?

MSSP partners are finding providers, finding receivers, or both.

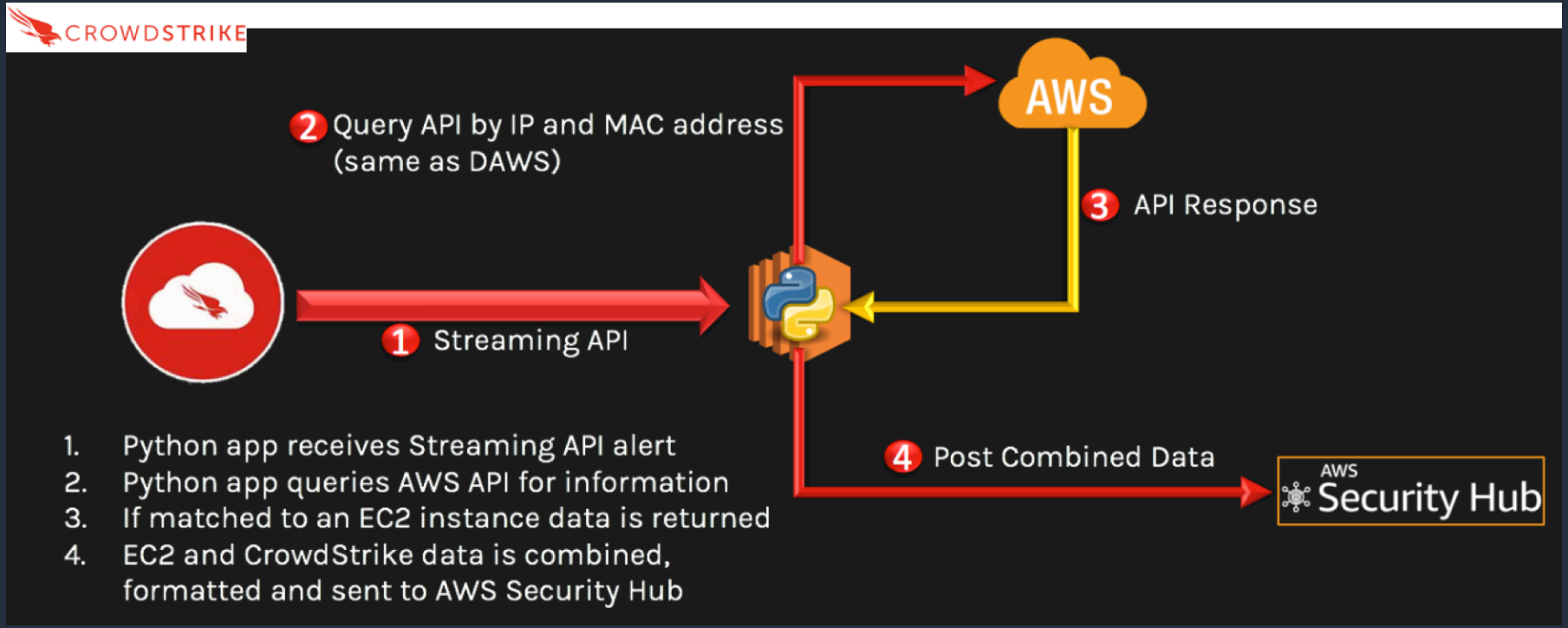
Non-MSSP consulting partners can also become Security Hub partners. They should submit two case studies on how they helped a specific customer do the following:

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

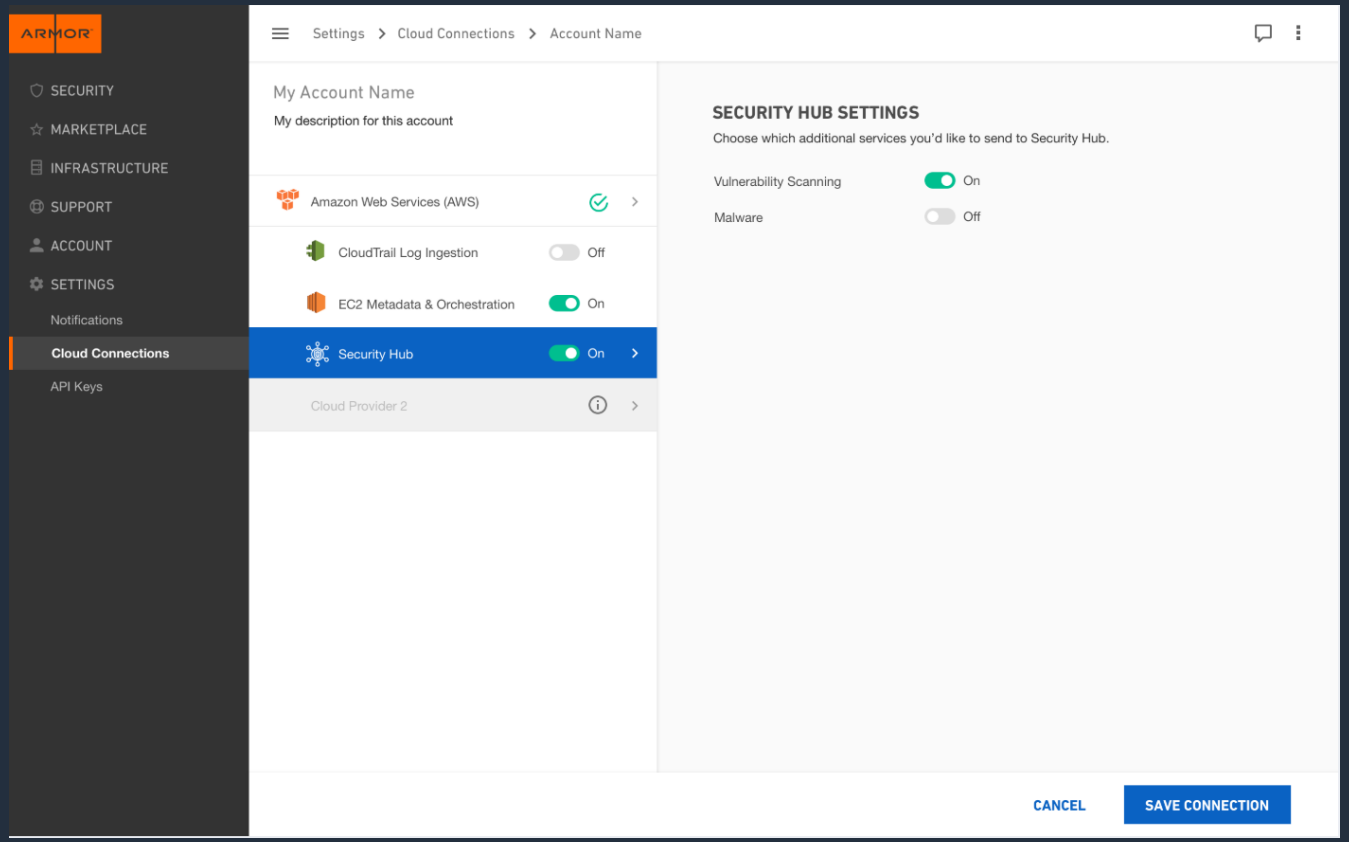
Two non-public case studies are required to become a Security Hub consulting partner.

aws

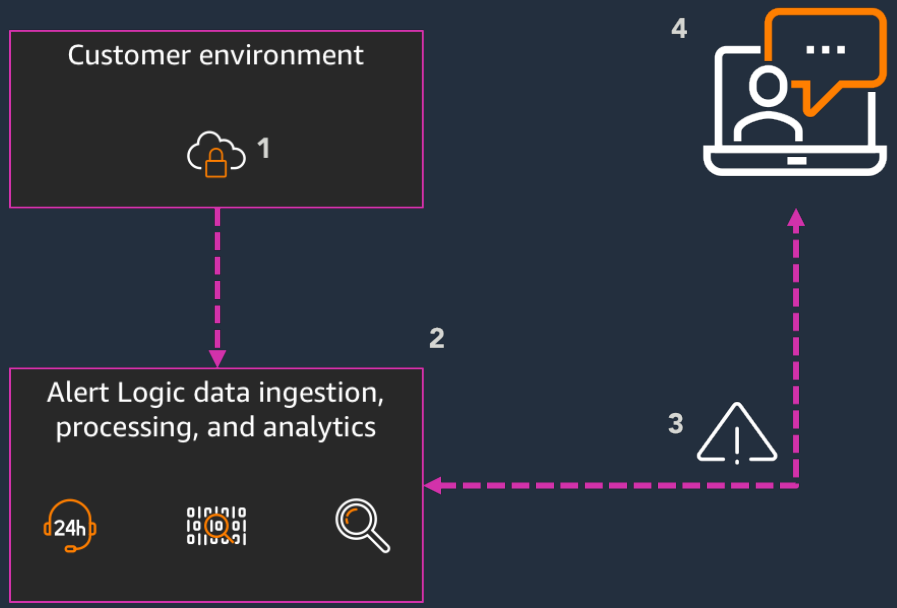
Partner integration examples — CrowdStrike



Partner integration examples — Armor

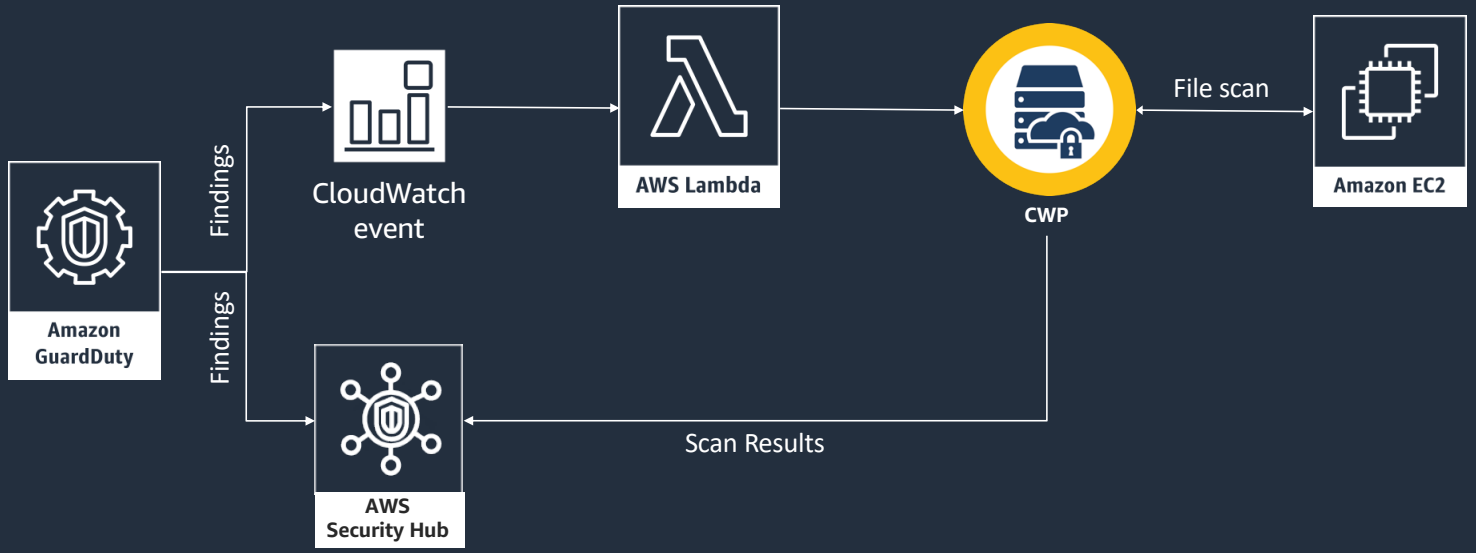


Partner integration examples — Alert Logic



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 — 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. Demo your integration to the Security Hub team.
8. Submit marketing information for approval (e.g., press release, blog, etc.)

Typically, this process takes 6-8 weeks end-to-end

aws

Agenda

Security Hub Partner Program Introduction

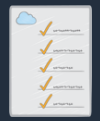
Security Hub Overview

Security Hub Demo

Next Steps

aws

Problem statement



Backlog of compliance requirements

1. Many compliance requirements and not enough time to build the checks

Too many security alert formats

2. Dozens of security tools with different data formats

Too many security alerts

3. Large volume of alerts and the need to prioritize and take action on

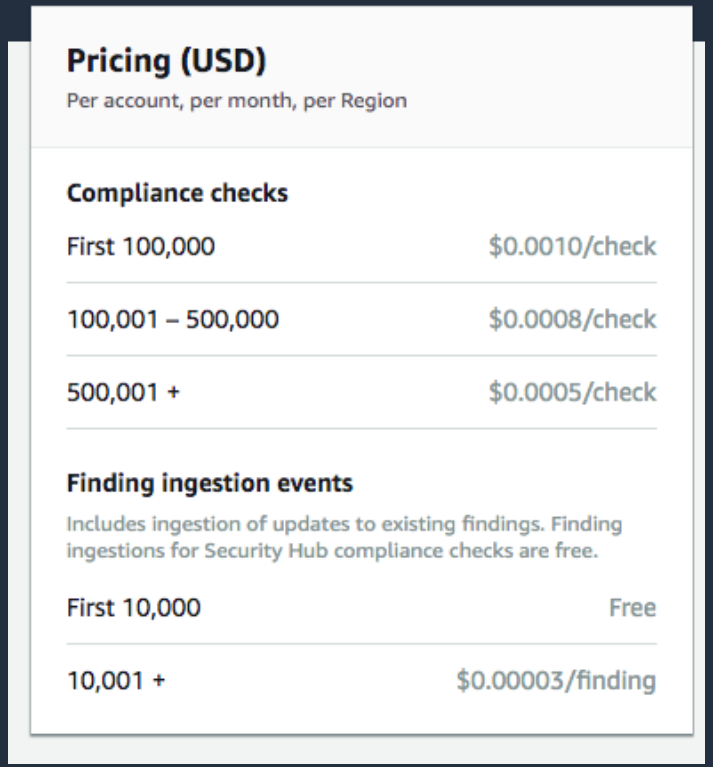
Lack of an integrated view

4. Lack of an integrated view of security and compliance across accounts

aws

AWS Security Hub overview

Rollout plans and pricing



Pricing (USD)

Per account, per month, per Region

Compliance checks

First 100,000	$0.0010/check
100,001 – 500,000	$0.0008/check
500,001 +	$0.0005/check

Finding ingestion events

Includes ingestion of updates to existing findings. Finding ingestions for Security Hub compliance checks are free.

First 10,000	Free
10,001 +	$0.00003/finding

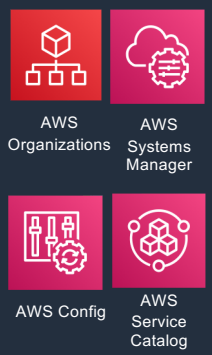
30-day free trial

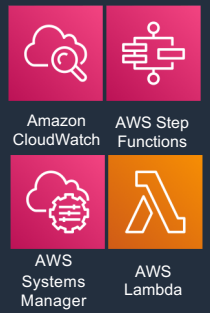
Supported Regions (18)

- Asia Pacific (Hong Kong)
- 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)
- EU (Stockholm)
- Middle East (Bahrain)
- South America (Sao Paulo)
- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)

aws

AWS Security-Related Services

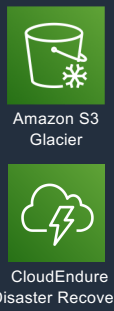




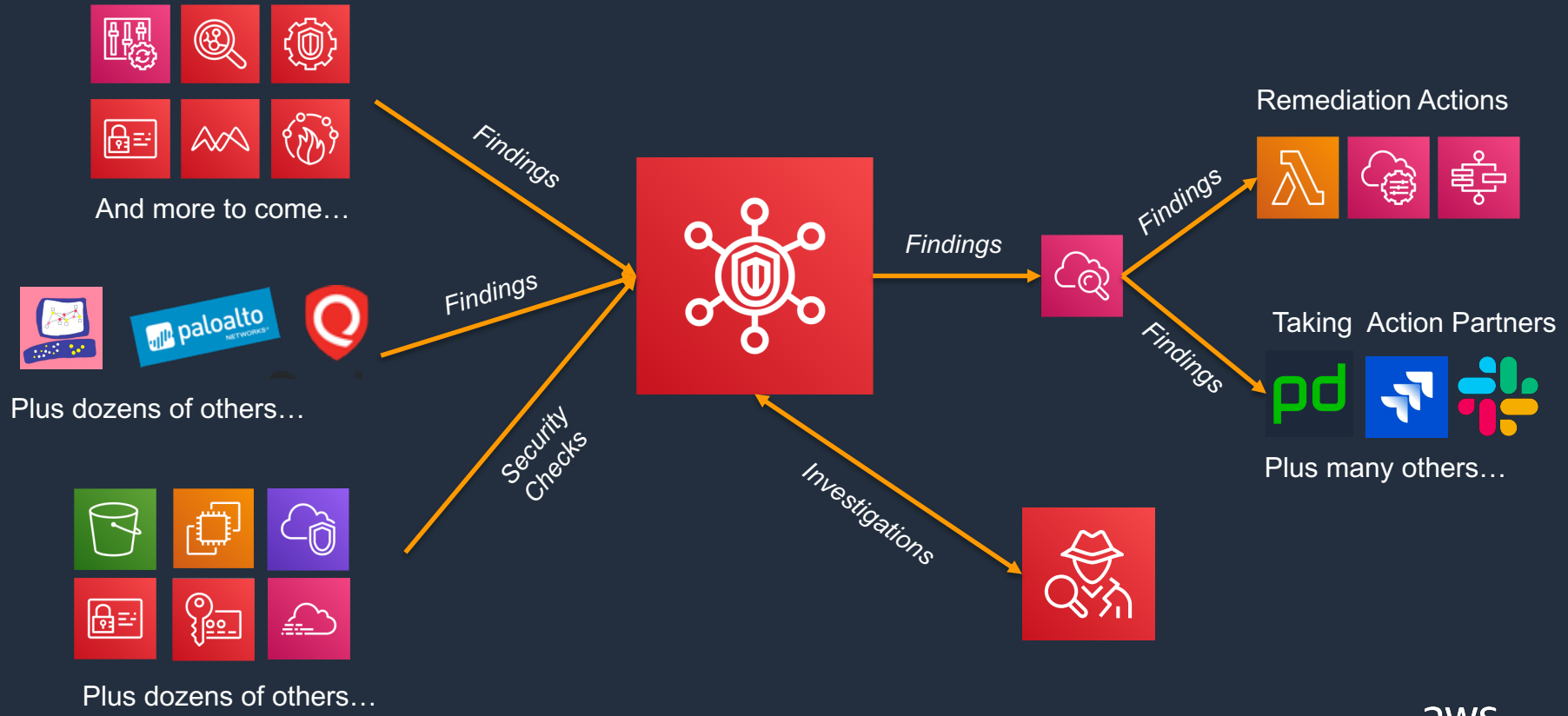
Identify → Protect → Detect → Respond → Recover

Automate

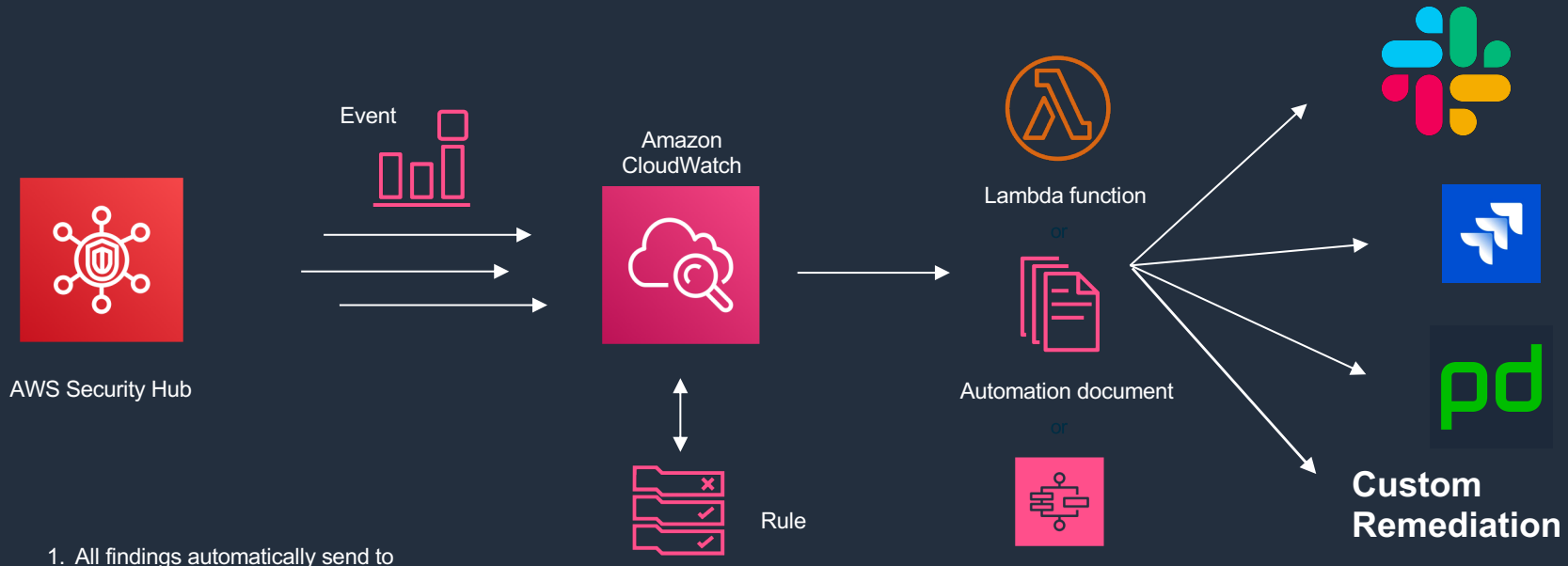
Investigate



AWS Security Hub Information Flows



Customizable response and remediation actions



1. All findings automatically send to CloudWatch events, **and**
2. Security Hub user can select findings in the console and take a custom action on them. These findings are sent to CloudWatch decorated with a custom action ID

3. User creates Amazon CloudWatch Events rules to look for certain findings associated with a custom action ID or findings with specific characteristics.

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

5. The target could be things like a chat, ticketing, on-call management, SOAR platform, or custom remediation playbook

Reference Customers

airbnb

edmunds

INTUIT

Frame.io

GoDaddy

here

THOMSON REUTERS®

move™

aws

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

aws

Use case 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

aws

Use case 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

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

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

securityhub-partners@amazon.com

securityhub-pms@amazon.com

https://join.slack.com/t/awssecurityhub/shared_invite/zt-dh0hphg1-sMy_133XHkurb0eqZKNRng

aws

Learning more

Try Security Hub for free: 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