



AWS Security Hub

Partner Program



Agenda

Security Hub Partner Program Introduction

Security Hub Overview

Security Hub Demo

Next Steps

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

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.

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

Partner integrations

Firewalls



Barracuda



Check Point
SOFTWARE TECHNOLOGIES LTD.



Endpoint



CROWDSTRIKE



Vulnerability



SOAR



TURBOT

splunk®

SIEM



IBM Security

splunk®

Compliance



SOFTWARE TECHNOLOGIES LTD.



Cloud Custodian

MSSP



Other



What about consulting partners?

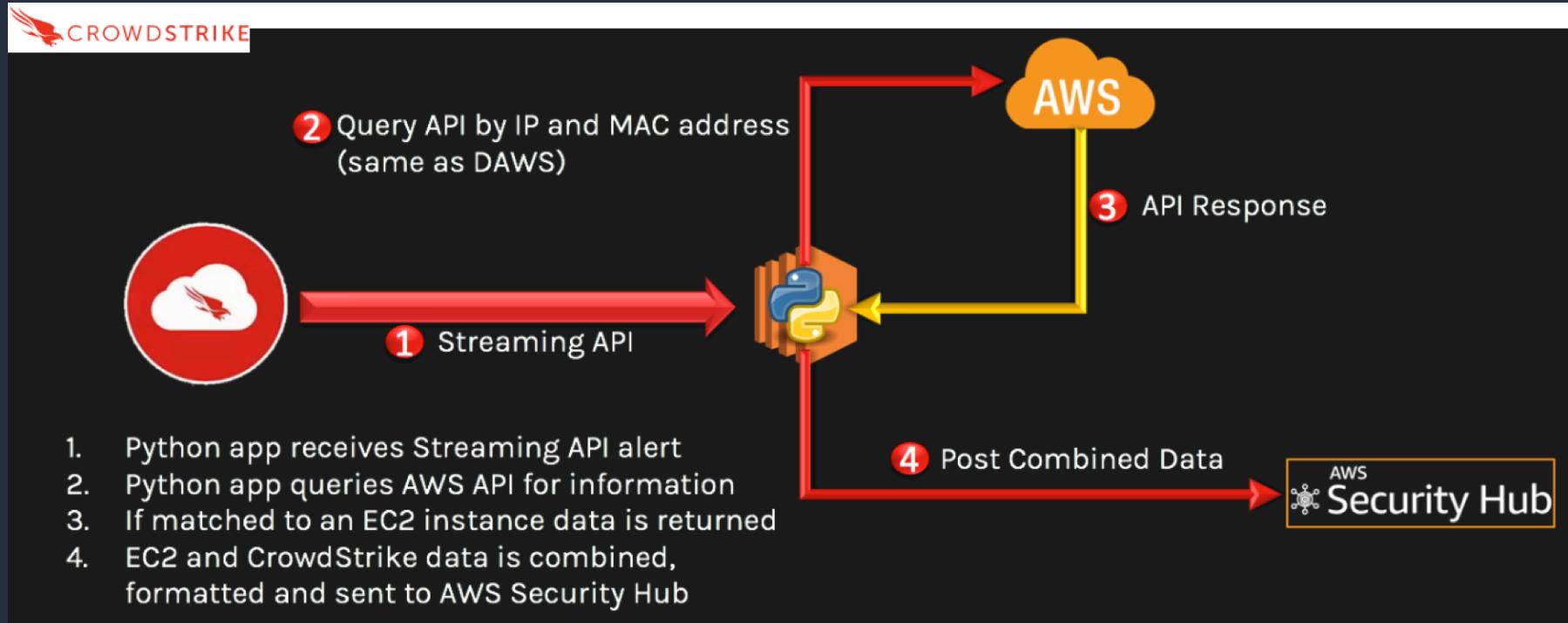
MSSP partners should must demonstrate how Security Hub would plug into their customer workflows (i.e., define the use case for your customers), as part of their technical integration with Security Hub.

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.

Partner integration examples — CrowdStrike



Partner integration examples — Armor

The screenshot shows the Armor platform's "Cloud Connections" settings page for "Account Name". The left sidebar includes options like SECURITY, MARKETPLACE, INFRASTRUCTURE, SUPPORT, ACCOUNT, SETTINGS, Notifications, Cloud Connections (which is selected and highlighted in orange), and API Keys.

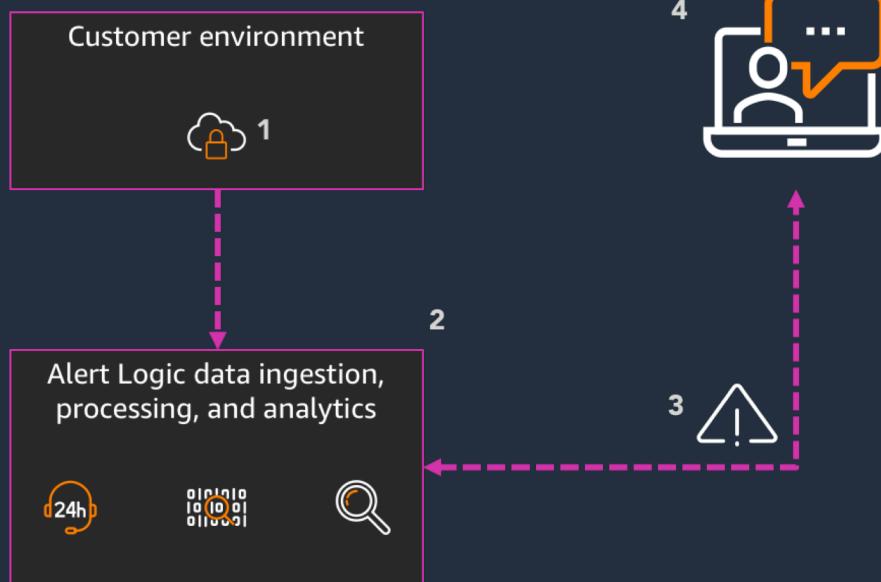
The main content area displays "My Account Name" and "My description for this account". Below this, under "SECURITY HUB SETTINGS", it says "Choose which additional services you'd like to send to Security Hub." with three toggle switches:

- Vulnerability Scanning: On (green switch)
- CloudTrail Log Ingestion: Off (gray switch)
- EC2 Metadata & Orchestration: On (green switch)
- Malware: Off (gray switch)

Below these settings, there are sections for "Amazon Web Services (AWS)" and "Security Hub" (which is also turned On). A section for "Cloud Provider 2" is partially visible at the bottom.

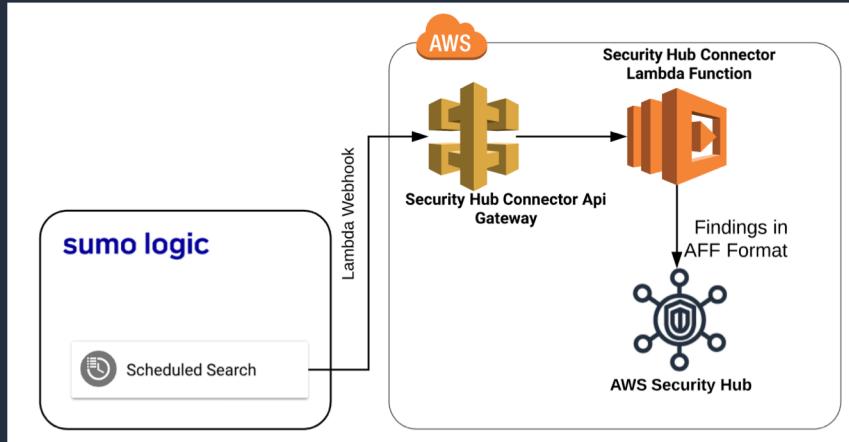
At the bottom right are "CANCEL" and "SAVE CONNECTION" buttons.

Partner integration examples — Alert Logic



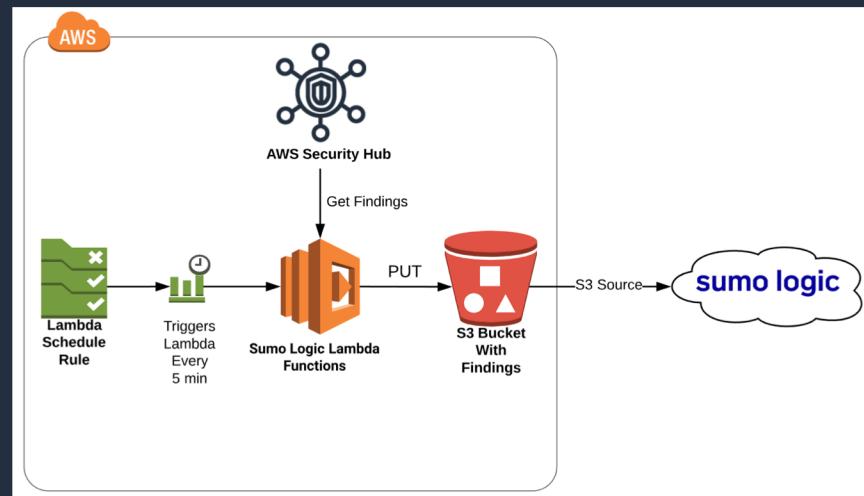
1. Inspected data is transported to Alert Logic's data ingestion, processing, and analytics platform
2. Alert Logic's **threat detection and response** capability analyzes the data and identifies **incidents**
3. An internal service (dedicated to AWS Security Hub) assesses the **incident** for potential 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

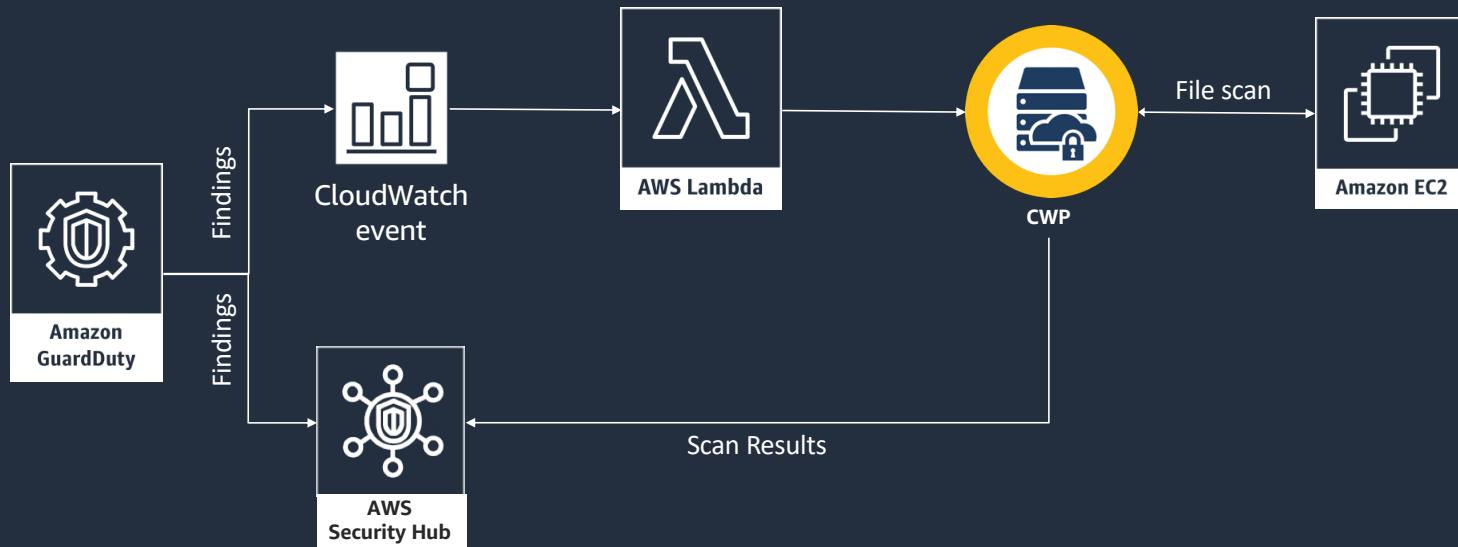


Sumo Logic sends findings to SecHub

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

Agenda

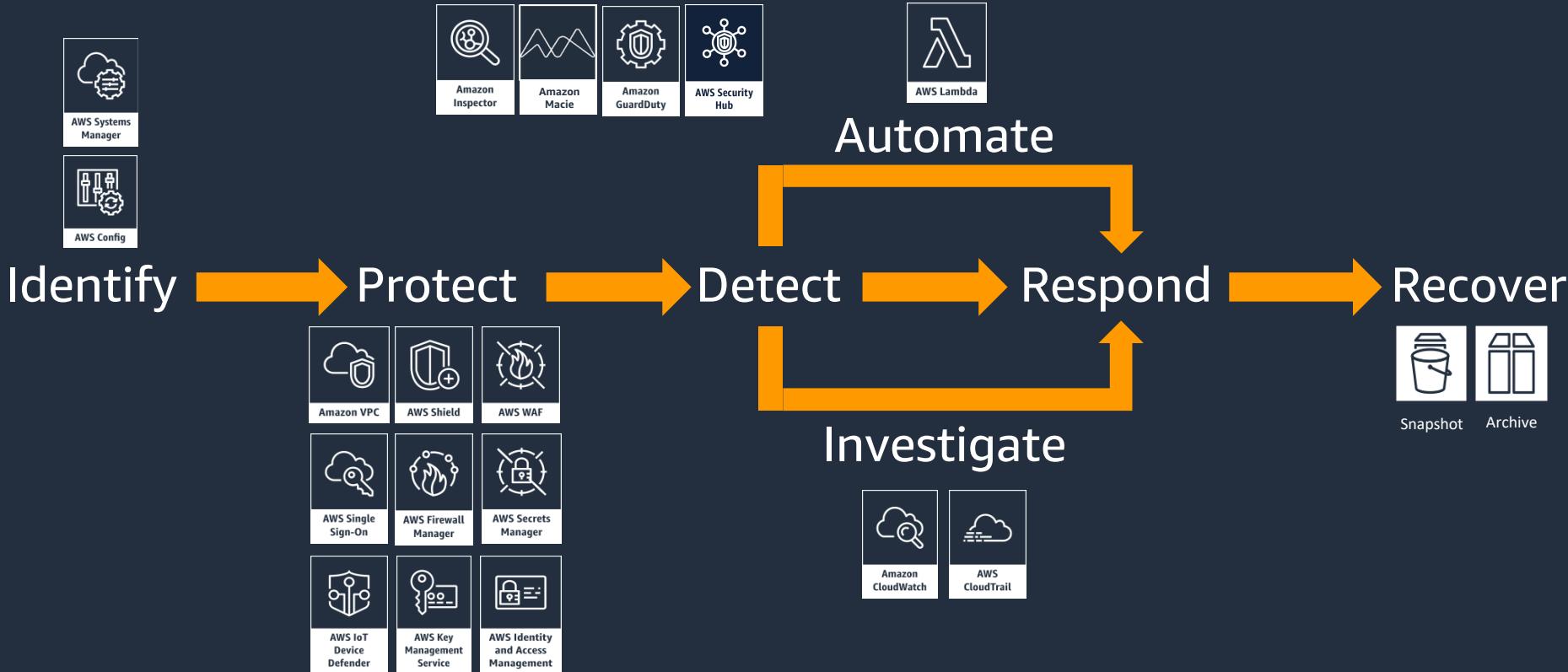
Security Hub Partner Program Introduction

Security Hub Overview

Security Hub Demo

Next Steps

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

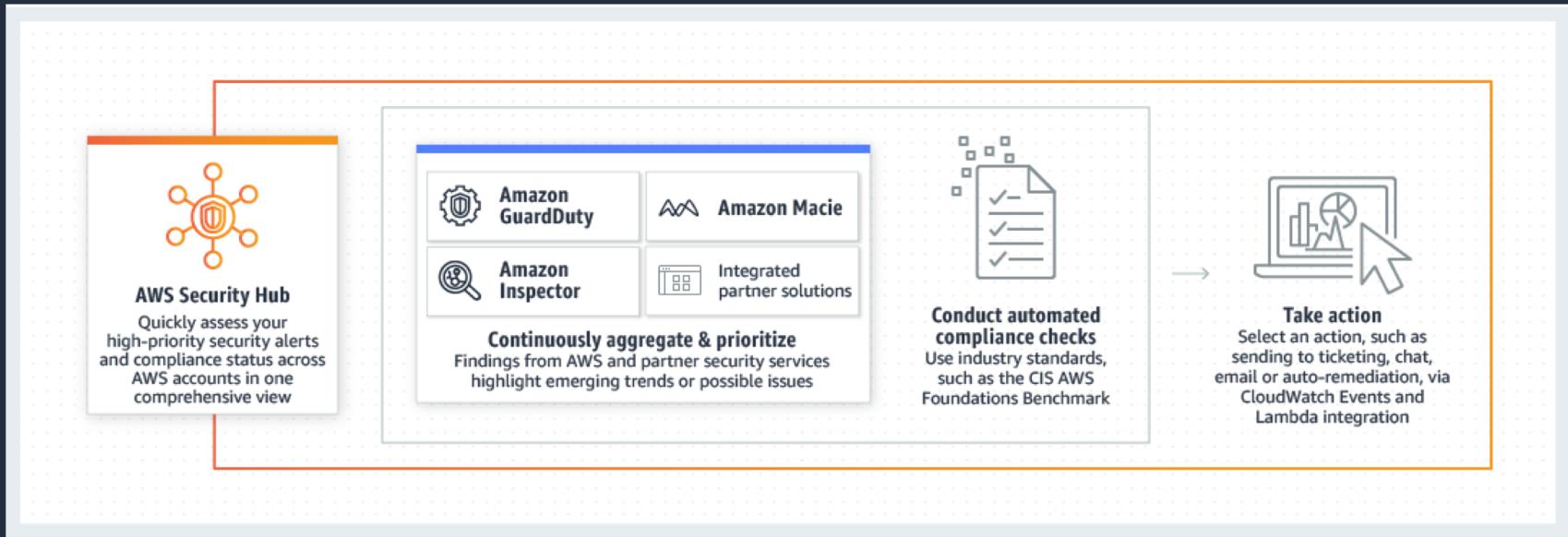
- 3 Large volume of alerts and the need to prioritize



Visibility

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

AWS 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)

A few clicks to enable Security Hub

Resource Groups

Admin/elykahn-isengard @ 52...

Security, Identity & Compliance

AWS Security Hub

Provides a comprehensive view of your AWS security and compliance posture

AWS Security Hub allows you to centrally view and manage security findings, automate compliance checks, and identify the highest priority security issues across your AWS environment.

How it works

The diagram illustrates the integration of AWS Security Hub with other AWS services:

- AWS Security Hub:** Displays high-priority security alerts and compliance findings across multiple AWS accounts in one comprehensive view.
- Amazon GuardDuty:** Continuously aggregate and prioritize findings from multiple AWS accounts to highlight emerging trends or possible issues.
- Amazon Inspector:** Conduct automated compliance checks using AWS Lambda functions such as the CIS AWS Foundations Benchmark.
- AWS Macie:** Take actions like selecting specific findings for remediation via email or auto-remediations, via CloudWatch Metrics, or via Lambda integrations.
- Integrated partner solutions:** Includes AWS Config items required for Security Hub's standards checks.

Benefits and features

Save time with aggregated findings	Improve compliance with automated checks
AWS Security Hub reduces the effort of collecting and prioritizing security findings across accounts, from AWS services, and AWS accounts using a central dashboard.	With AWS Security Hub, you can run automated, continuous account-level configuration and compliance checks based on AWS CloudFormation stacks, AWS Lambda functions, and AWS CloudWatch Metrics.

AWS Security Hub Setup

Begin aggregating and prioritizing findings by conducting compliance checks.

[Enable Security Hub](#)

Pricing (US)

Pricing is under development and AWS Security Hub is free during the preview period. AWS Config Config Items (not Config Rules) is required for Security Hub's standards checks, and it is priced separately. Not already using AWS Config, see the [Config page](#) for pricing of Config Items. You will be charged for Config Rules created by Security Hub; they are included in Security Hub pricing. See pricing will be provided later during the public period.

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](#)

[Cancel](#) [Enable AWS Security Hub](#)

Simple multi-account setup

Member accounts							Actions ▾			
Member accounts share their findings with you. Members must first accept your invitation. Learn more										
Viewing : All: 8		+ Add accounts								
<input type="checkbox"/>	Account ID	▲	Email	▼	Status	▼	Date Invited	▼	Date Updated	▼
<input type="checkbox"/>	[REDACTED]		not-specified@amazon.com		Enabled		11-19-2018 16:00:00		11-19-2018 16:00:00	
<input type="checkbox"/>	[REDACTED]		[REDACTED]		Enabled		11-18-2018 17:15:30		11-18-2018 19:29:27	
<input type="checkbox"/>	[REDACTED]		[REDACTED]		Enabled		11-25-2018 21:27:07		11-25-2018 22:35:08	
<input type="checkbox"/>	[REDACTED]		[REDACTED]		Enabled		11-20-2018 18:35:11		11-20-2018 18:35:45	
<input type="checkbox"/>	[REDACTED]		[REDACTED]		Invited (12 hours ago)		11-25-2018 13:45:28		11-25-2018 13:45:28	X
<input type="checkbox"/>	[REDACTED]		[REDACTED]		Invited (5 days ago)		11-21-2018 13:57:42		11-21-2018 13:57:42	X
<input type="checkbox"/>	[REDACTED]		not-specified@amazon.com		Enabled		11-19-2018 16:00:00		11-19-2018 16:00:00	
<input type="checkbox"/>	[REDACTED]		supervpc-test@amazon.com		Enabled		11-20-2018 13:26:53		11-20-2018 17:19:23	

AWS Security Finding Format

~100 JSON-formatted fields

Severity.Normalized

Finding Types

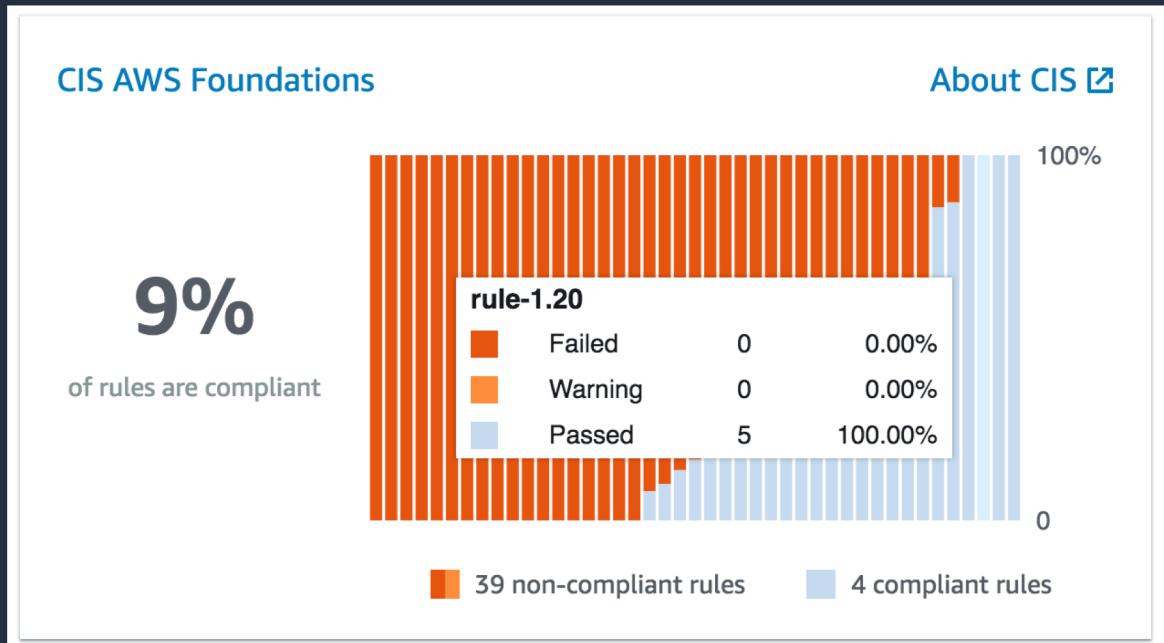
- Sensitive Data Identifications
- Software and Configuration Checks
- Unusual Behaviors
- Tactics, Techniques, and Procedures (TTPs)
- Effects



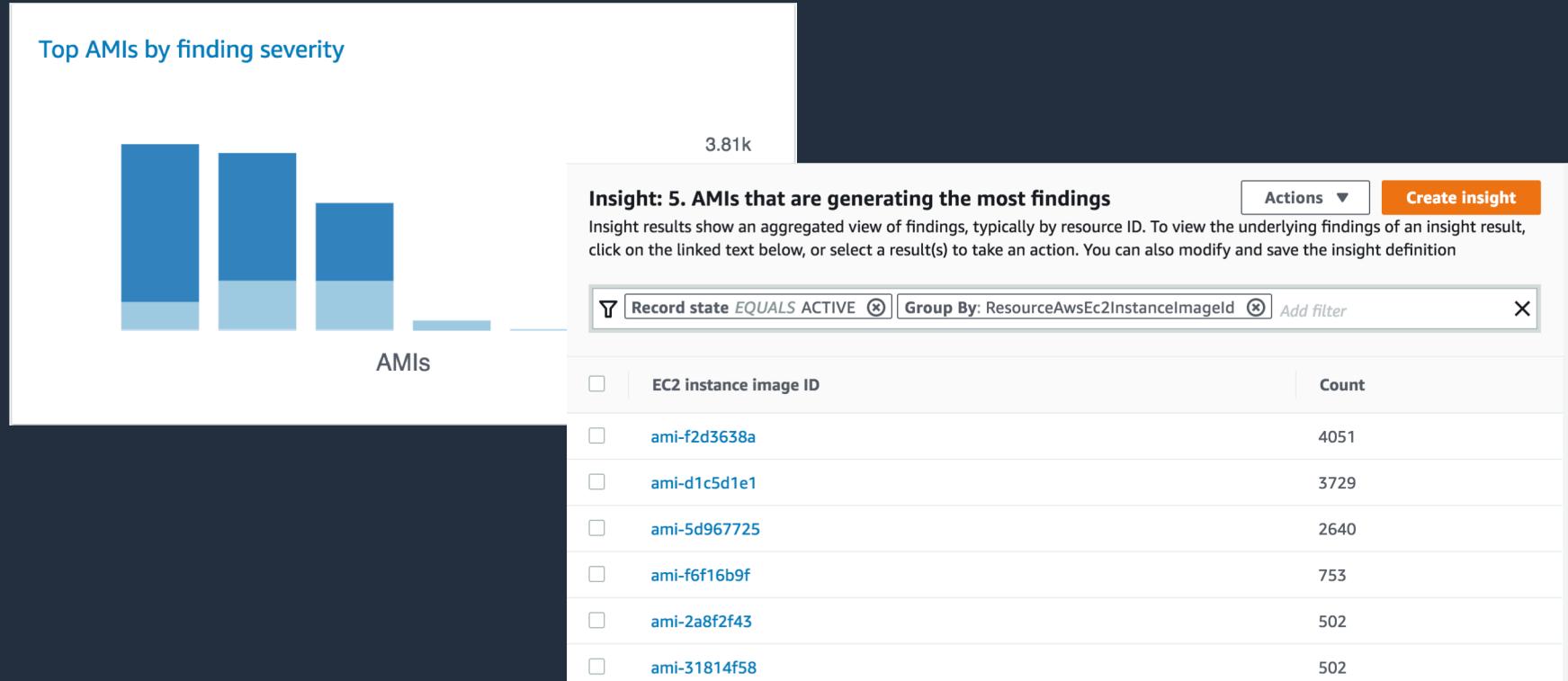
Automated compliance checks



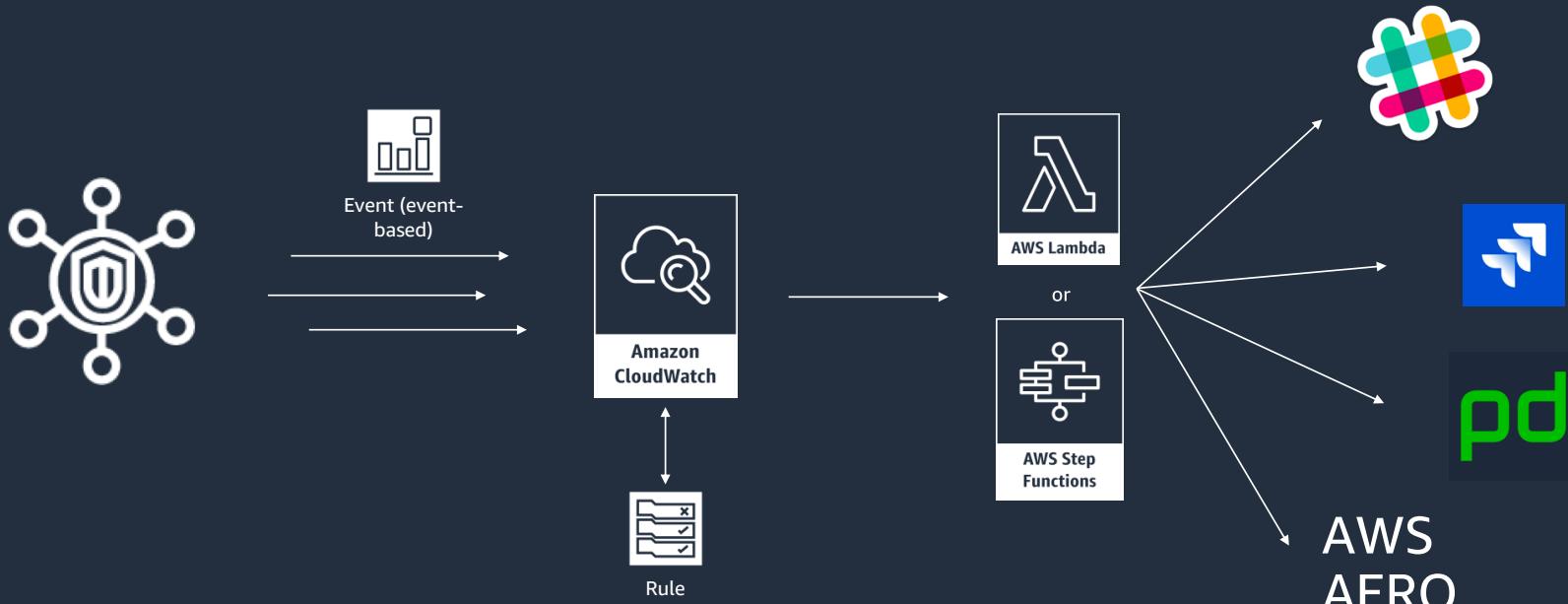
43 fully automated,
nearly continuous
checks



Insights help identify resources that require attention



Customizable response and remediation actions



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

Agenda

Security Hub Partner Program Introduction

Security Hub Overview

Security Hub Demo

Next Steps

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

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