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 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.
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
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.
Partner integration examples — CrowdStrike

1. Python app receives Streaming API alert
2. Python app queries AWS API for information
3. If matched to an EC2 instance data is returned
4. EC2 and CrowdStrike data is combined, formatted and sent to AWS Security Hub
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

Amazon GuardDuty → Findings

CloudWatch event → Findings

AWS Lambda → CWP

File scan → Amazon EC2

AWS Security Hub → Scan Results
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).
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
Agenda

Security Hub Partner Program Introduction

Security Hub Overview

Security Hub Demo

Next Steps
Problem statement

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

2. Too many security alert formats
   - Dozens of security tools with different data formats

3. Too many security alerts
   - Large volume of alerts and the need to prioritize and take action on

4. Lack of an integrated view
   - Lack of an integrated view of security and compliance across accounts
AWS Security Hub overview

AWS Security Hub
Quickly assess your high-priority security alerts and compliance status across AWS accounts in one comprehensive view

Continuously aggregate & prioritize
Findings from AWS and partner security services highlight emerging trends or possible issues

Conduct automated compliance checks
Use industry standards, such as the CIS AWS Foundations Benchmark

Take action
Investigate findings and/or take response and remediation actions
Rollout plans and pricing

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)

30-day free trial

<table>
<thead>
<tr>
<th>Compliance checks</th>
<th>Pricing (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>First 100,000</td>
<td>$0.0010/check</td>
</tr>
<tr>
<td>100,001 – 500,000</td>
<td>$0.0008/check</td>
</tr>
<tr>
<td>500,001 +</td>
<td>$0.0005/check</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Findings</th>
<th>Pricing (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>First 10,000</td>
<td>Free</td>
</tr>
<tr>
<td>10,001 +</td>
<td>$0.00003/finding</td>
</tr>
</tbody>
</table>
AWS Security-Related Services

Identify -> Protect -> Detect -> Automate -> Respond -> Recover

AWS Organizations
AWS Systems Manager
AWS Config
AWS Service Catalog

AWS Transit Gateway
AWS VPC
Amazon VPC
Amazon Cloud Directory

Amazon GuardDuty
Amazon GuardDuty
AWS IoT Device Defender

Amazon Inspector
AWS Security Hub
AWS Trusted Adviser
AWS Well-Architected Tool

AWS Config
String Manager
AWS Step Functions

AWS Single Sign-On
AWS WAF
IAM
AWS Secrets Manager
KMS
Amazon Cognito
AWS Control Tower

AWS Direct Connect
Resource Access manager
AWS Directory Service

Amazon CloudWatch
Amazon CloudWatch
AWS Systems Manager
AWS Lambda

AWS Direct Connect
AWS WAF
AWS Firewall Manager
AWS Certificate Manager
AWS CloudHSM
AWS Single Sign-On

AWS Step Functions
AWS Step Functions
AWS CloudFormation
AWS OpsWorks

Amazon S3
Glacier
CloudEndure
Disaster Recovery

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
AWS Security Hub Information Flows

Findings

Security Checks

Investigations

Remediation Actions

Taking Action Partners

Plus dozens of others…

And more to come…

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
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

AWS Security Hub

Customizable response and remediation actions
# Use case 1: Centralized security and compliance workspace

<table>
<thead>
<tr>
<th><strong>Goal</strong></th>
<th>Have a single pane of glass to view, triage, and take action on AWS security and compliance issues across accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personas</strong></td>
<td>SecOps, compliance, and/or DevSecOps teams focused on AWS, Cloud Centers of Excellence, the first security hire</td>
</tr>
</tbody>
</table>
| **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 |
### Use case 2: Centralized routing to a SIEM

<table>
<thead>
<tr>
<th>Goal</th>
<th>Easily route all AWS security and compliance findings in a normalized format to a centralized SIEM or log management tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personas</td>
<td>SecOps, compliance, and/or DevSecOps teams</td>
</tr>
</tbody>
</table>
| 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 |
Use case 3: Dashboard for account owners

<table>
<thead>
<tr>
<th>Goal</th>
<th>Provide visibility to AWS account owners on the security and compliance posture of their account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personas</td>
<td>AWS account owners</td>
</tr>
</tbody>
</table>
| 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 |
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

securityhub-partners@amazon.com

securityhub-pms@amazon.com

https://join.slack.com/t/awssecurityhub/shared_invite/zt-dh0hphg1sMy_133XHkurb0eqZKNRng
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