Security Hub Partner Onboarding Guide

Introduction

This document is intended for Amazon Web Services (AWS) partners who are exploring creating an integration to send security findings into the AWS Security Hub service. The Security Hub service is different from many other AWS services because partners are able to send information into the service, vs. the traditional model of pulling information from a service. Partners will not be able to send information into a customer's Security Hub until they have been enabled as a provider by the Security Hub team. To ensure that the customer and partner experience with Security Hub is positive there are a series of onboarding steps that a partner must go through before they can be enabled as a provider in Security Hub. This document will outline the onboarding steps that a partner needs to follow to send security findings to Security Hub. Additionally, this document will provide additional details related to a Security Hub integration to provide color around the integration steps.

Along with this document you should have also received the following documents:

- Security Hub provider integration FAQ
- Security Hub resource policy approach
- Partner Manifest for Security Hub
- Partner First Call Deck

It is recommended that partners read the onboarding guide and the integration FAQ first.

There are multiple ways that partners can integrate with Security Hub:

1. Sending findings to Security Hub
2. Consuming findings from Security Hub
3. Partners who both send and consume findings to / from Security Hub
4. Partners who use Security Hub as the center of a Managed Security Service Provider (MSSP) offering
5. Partners who consult AWS customers on how to deploy and operationalize Security Hub
6. Partners who do multiple options above

This onboarding guide will primarily focus on partners pushing findings into Security Hub.

There are three major things that a partner needs to do to send security findings to Security Hub:

1. Map partner security findings to the AWS Security Finding Format (ASFF).
2. Build your integration architecture to push findings to the correct regional Security Hub endpoint. This involves defining if you will be sending findings from your own AWS account or from within the customer's account(s) and whether you will be using cross-account policies or relying on customers to put resource policies in place.

3. The customer (or the partner acting on behalf of the customer via cross-account roles) "subscribes" your product to the customer's account, which puts in place resource policies needed to accept findings from that product for that account.

Open source examples of integrations built to work with Security Hub:

- https://aws.amazon.com/blogs/opensource/announcing-cloud-custodian-integration-aws-security-hub/
- https://aws.amazon.com/blogs/security/use-aws-fargate-prowler-send-security-configuration-findings-about-aws-services-security-hub/
- https://aws.amazon.com/blogs/security/how-to-import-aws-config-rules-evaluations-findings-security-hub/

For partners looking to receive findings from Security Hub this integration can be accomplished in one of two ways:

1) All findings are automatically sent to CloudWatch events. A customer can create specific CloudWatch event rules to send findings to specific targets (e.g., a SIEM, a S3 bucket, etc.).

2) Security Hub allows customers to select specific findings or groups of findings from within the console and take action on them (e.g., send to a SIEM, ticketing system, chat platform, or remediation workflow). This would be part of an alert triage workflow that a customer is performing within Security Hub. These are called custom actions. When a user takes a custom action, a CloudWatch Event is created for those specific findings. A partner could leverage this capability and build out CloudWatch Event rules/targets for a customer to use as part of a custom action. Note that this capability is not for automatically sending all findings of a particular type or class to CloudWatch Events. It is for a user taking action on a specific finding(s).

Here are two blog posts outlining solutions that leverage integration with Security Hub and CloudWatch events for custom actions:

- https://aws.amazon.com/blogs/apn/how-to-integrate-aws-security-hub-custom-actions-with-pagerduty/
- https://aws.amazon.com/blogs/apn/how-to-enable-custom-actions-in-aws-security-hub/
- https://aws.amazon.com/blogs/security/how-to-import-aws-config-rules-evaluations-findings-security-hub/

Why do a Security Hub Integration?

AWS Security Hub gives customers a comprehensive view of their high-priority security alerts and compliance status across AWS accounts. A key feature of Security Hub is the ability for partners to send security findings to Security Hub so that a customer has insight into the security findings for their AWS accounts, that are generated by their partners.

As an AWS partner there are several different ways that an integration with Security Hub can add value:

1) Your customers are asking for a Security Hub integration.
2) Integrating with Security Hub adds visibility to your customers for a single view of their AWS security related findings.
3) Integrating with Security Hub provides an opportunity to have new customers discover your solution when looking for partners who provide findings around certain types of security events.

Before you begin building an integration with Security Hub it is highly recommended that you assess the reasons for why you are building a Security Hub integration. Past experience has shown that having input from your customers that they desire a Security Hub integration with your product helps in making a successful integration. While doing an integration in an effort to position your company purely for marketing reasons and to acquire new customers is also an option, doing the integration without any current customer input may not yield the results you are expecting if you are not doing this with customer needs in mind.

Security Hub Learning Materials

The following materials will help you get a better understanding of what the AWS Security Hub solution is and how AWS customers can use the service. We encourage you to review these materials to get a better understanding of the Security Hub Service. Additionally, we encourage you to turn on Security Hub in one of your AWS accounts and get some hands on time with the service.

- Introduction to AWS Security Hub: https://www.youtube.com/watch?v=o0NDi01YPXs
- Security Hub user guide: https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html
- Security Hub API reference: https://docs.aws.amazon.com/securityhub/1.0/APIReference/Welcome.html
- Onboarding webinar: https://pages.awscloud.com/aws-security-hub-partners-onboarding.html

Partner Pre-Requisites

Before beginning an integration with Security Hub the partner must meet the following requirements:

1) Partner must be in good standing and at the Select level or higher as an AWS Amazon Partner Network (APN) partner.
2) Partner must have a Mutual Non-Disclosure Agreement in place with AWS.

Partner Onboarding Process

These are the high level steps that a partner should expect to go through as part of their onboarding process for being able to send security findings to Security Hub.

1) Partner initiates an engagement with the AWS Partner team or Security Hub team, expressing interest in becoming a partner to Security Hub. Partner identifies which email addresses should be added to Security Hub communication channels.
2) AWS provides the partner with the Security Hub Partner onboarding materials.
3) Partner is invited to the Security Hub partner Slack channel where they can ask questions related to their integration.
4) Partner provides AWS partner contacts with a draft Manifest for review. This initial review does not have to have all the Manifest details complete, but it should at least contain use case and dataset information.
5) Security Hub team provides the partner with a Product Amazon Resource Name (ARN) for their product, which the partner will use to send findings to Security Hub.
    a. For more information see: https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-providers.html
6) Partner builds their integration to send and/or receive findings to/from Security Hub, including mapping their findings to the AWS Security Finding Format if sending findings.
7) Partner demos integration to the Security Hub product team. This integration should be demonstrated against an account that the Security Hub team owns and cover both setup and usage of the integration. Please contact the Security Hub team for details. Hub team gives approval to move forward with listing the partner as a provider if they are comfortable with the integration.
8) Partner provides a final manifest that includes documentation links, logos, and final wording for the description. If the documentation link is behind a login screen, please send a pdf of the documentation for review.
9) Partner provides a short demo video of the working integration that can be leveraged for marketing purposes. Partner also provides a one slide architecture diagram that can be incorporated into the Security Hub first call deck.
10) Security Hub team creates provider integration in the Security Hub console, enabling customers to discover and enable integrations with the partner.
11) Partner optionally engages in additional marketing efforts to promote their Security Hub integration. See the Go-To-Market section of this document for more details.

Partner Manifest

The partner manifest contains information that will be used to create your partner product ARN for integrating with Security Hub. This manifest will provide the Security Hub team with information that will be used to populate your partner provider page in the Security Hub console and to populate the Security Hub insight library with your proposed default insights related to your integration. See the **Product Information Manifest for Security Hub Console.docx** document for further details.

AWS Security Finding Format

The *AWS Security Finding Format* (ASFF) provides a consistent description of findings that can be shared between AWS security services, partners, and end-customer's own security systems. This reduces integration efforts, encourages a common language, and provides a blueprint for implementors. ASFF is the required wire protocol format for communicating findings with Security Hub via API. Findings are represented as JSON documents that adhere to the ASFF JSON Schema and RFC-7493 The I-JSON Message Format.

Both new and updated findings must be sent to Security Hub using the BatchImportFindings API, refer to the guidance below for design and ASFF mapping principles.

Building and Testing a Security Hub Integration

Once you have received your ARN for Security Hub, all of the testing for your integration can be completed against an AWS account that you own. This will allow you full visibility into how the findings are showing in Security Hub and will give you an understanding of the experience that a customer will have with your security findings.

Throughout the build of a Security Hub integration partners are encouraged to keep their AWS partner contacts in the loop on how their integration is going and leverage their AWS partner contacts for help with integration questions.

Go-To-Market Activities

Being Listed as a Security Hub Partner

Once you have been approved as a Security Hub partner your solution can be displayed on the Security Hub partner page (https://aws.amazon.com/security-hub/partners/). To be listed on this page please provide the following details as part of your submitted partner manifest:

1) Brief description of your solution, its integration with Security Hub, additional value add that the integration with Security Hub is providing to customers. Please limit this to 700 characters including spaces.
2) URL to a page describing your solution. It is recommended that this site be one that is specific to your AWS integration and more specifically your Security Hub integration. The site should focus on the customer experience and value customers receive in leveraging their capabilities.
3) High resolution copy of your logo. 600x300 pixels. See manifest for more detailed requirements.

Demo Video

Partners should produce a demo video of the working integration that can be leveraged for marketing purposes. These should be hosted on your video platform account, but we will link to these from our partner page.

Architecture Slide

Partners should produce a single slide that includes an architecture diagram for how your solution integrates with Security Hub. We will include this in our Security Hub first call deck.

Press Release

Once a partner has been approved as a provider for Security Hub a partner may optionally publish a press release on their website and/or PR channel(s) with AWS approvals. Prior to publishing the press release partners need to submit this press release to AWS so that AWS partner marketing, Security Hub leadership, and AWS External Security Services (ESS) can review. As part of this press release the partner can propose a quote for Dan Plastina, VP Security Services. Please work with your Partner Development Manager (PDM) to initiate this process. We have a 10 business day SLA for reviewing press releases.

AWS Partner Network Blog

We can also assist in putting up a blog post authored by you on the AWS Partner Network Blog. If interest, please contact your Partner Development Manager or Partner Solution Architect to begin the process. Please note that the blog must focus on a customer story and use case and not positioned solely around being an integration launch partner. Additionally, please note that APN Blogs can take in upwards of 8 weeks for final approval and publishing.

7 Key Things to Know About the APN Blog:

- **Partner posts should be educational and provide deep expertise** on a topic relevant to AWS customers.
- **Limit of 3 posts per partner per year:** With tens of thousands of APN Partners, we must be equitable in our coverage.
- **Advanced or Premier Tier partners only:** Exceptions for Select partners with an APN program designation such as Service Delivery.
- **Sponsors required for technical content:** Posts must have a technical sponsor who can validate the solution or use case.
- **Content should be original to the APN Blog:** Not repurposed from existing blog posts, whitepapers, etc.

- **4-6 weeks needed for editing:** This is from the moment the first full-length draft is submitted.
- **1,500 words is the ideal story length:** Readers value deep, educational content that teaches them what's possible on AWS.

Why Write for the APN Blog?

- **Credibility:** For APN Partners, having a story published by AWS can influence customers globally.
- **Visibility:** The APN Blog is one of the most-read blogs at AWS with 1.79M page views in 2019, including influenced traffic.
- **Business:** APN Partner posts have "connect" buttons that can generate leads via the ACE Platform.

What Kind of Content is the Best Fit?

- **Technical content is the most popular type of story we can share**. This includes solution spotlights and how-tos. More than 75% of readers are looking at this technical content.
- **Customers value 200-level or above stories** that demonstrate "how" something works on AWS or "how" an APN Partner solved a business problem for customers.
- **Posts written by technical experts or SMEs** perform the best by far. Basically, not marketing people. :)

Slick Sheet / Marketing Sheet

If you create a one-page slick sheet outlining your product, its integration architecture, and joint customer use cases, please send a copy to the Security Hub team. We will add these to our partner page.

White Paper / e-Book

If you create a white paper or e-Book outlining your product, its integration architecture, and joint customer use cases, please send a copy to the Security Hub team. We will add these to our partner page.

Webinar

If you do conduct a webinar about your integration, please send us a recording of the webinar, and we will link to it from the partner page. We are also happy to participate in your webinar with a Security Hub subject matter expert.

Approvals and Marketing Funds

If you want to create your own marketing contents related to AWS Security Hub you should send a draft to your AWS partner manager for review and approval before releasing these contents to make sure everyone is aligned on messaging.

APN partners can leverage APN Partner Marketing Central and the Market Development Funds (MDF) program to create campaigns and get funding support. Please consult your partner manager for details about these programs.

Additional Resources

- Script to automate the process of running the Security Hub multi-account workflow across a group of accounts: https://github.com/awslabs/aws-securityhub-multiaccount-scripts