

# Product Integration Manifest

## Use Case and Marketing Information

**Instructions:** Please submit this Word document back to the Security Hub team with the information request below. Use red text to denote your answers. We will use this information to create your website listing, product card and to inform the product team of your use case.

Refer to **Appendix A – Product Readiness Checklist** to evaluate the quality of your proposed integration along with what information you provide. All technical information provided must also be reflected in your documentation. We will use this checklist to determine whether your integration is ready to be launched.

### **Finding Providers & Consumers Use Case | Required if ISV**

Please describe your use case around your integration with Security Hub by answering the following questions, if you won't be sending or receiving findings note that here and complete the next section. This information must be reflected in your documentation:

- Will you be sending findings, receiving findings, or both?
- If sending findings, what types of findings and are you sending all findings or a certain subset of findings?
- If receiving findings, what will you be doing with those findings and what types of findings (e.g. all findings, findings of a certain type, or only specific findings that a customer selects) will you receive?
- Will you be updating findings and, if so, which fields? We recommend updating findings, as it helps decrease findings noise for customers. Updating findings is accomplished, by sending a finding that has a finding ID associated with a finding that you have already sent.

*Feel free to get early feedback on use case and datasets by reaching out to the the AWS Partner or Security Hub team.*

### **Consulting Partner (CP) Use Case | Required if CP**

Please provide two customer use cases around regarding your work with Security Hub. These can be private use cases. We will not advertise them anywhere. They should describe either or both of the following actions:

- How you help customers **bootstrap** Security Hub (e.g. via professional services, Terraform module/CloudFormation template, etc.)
- How you help customers **operationalize and extend** Security Hub (e.g. providing response/remediation templates, building custom integrations, setting up executive dashboards via BI tools, etc.)

### **Datasets | Required**

Provide what finding(s) your product produces in their native format (JSON, XML, etc.) that you will be sending to Security Hub, as well as an example of how you will be mapping the

finding(s) into the [AWS Security Finding Format \(ASFF\)](#). *Please let us know if you need any updates to the ASFF to support your integration.*

### **Architecture | Required**

Please describe how you will integrate with Security Hub. This must be reflected in your documentation as well. Architecture diagrams are required.

- What AWS Services, OS agents, etc. will you be using?
- For sending findings, will you send findings from the customer or your own AWS account?
- For receiving findings, describe how you will use the CloudWatch Event integration
- How will you transform findings to ASFF?
- How will you batch up findings, retain state, and avoid throttling limits?

### **Configuration | Required**

Please describe how a customer will configure your integration with Security Hub. CloudFormation templates (or similar Infrastructure as Code templates) are required at a minimum, but some partners have gone beyond that with a UI that supports “one-click” integration. Configuration should take no more than 15 minutes. Configuration guidance must be provided in your product documentation for your integration as well.

### **Average findings per day per customer | Required if finding provider**

How many finding updates per month (average and max) do you expect to send to Security Hub across your customer base? Orders of magnitude estimates are acceptable.

### **Latency | Required if finding provider**

How quickly will you batch up and send findings to Security Hub (i.e. what is the latency from when the finding is created in your product to when it is sent to Security Hub?) This information must be reflected in your product documentation for your integration, as it is a common question we get from customers.

### **Company and product description | Required**

This should briefly describe your company and product with a specific emphasis on the nature of your Security Hub integration. We will use this on our /security-hub/partners/ page. If you are integrating multiple products with Security Hub, you can have separate descriptions for each product that you are integrating, but we will combine them into a single entry on the partner page. **No more than 700 characters with spaces.**

### **Partner website assets | Required**

At a minimum you must provide a URL that we will use for the Learn More hyperlink on /security-hub/partners/ page. It should be a marketing landing page that describes the integration between your product and Security Hub. If you are integrating multiple products with Security Hub, you could have a single landing page for them. We recommend linking to your configuration instructions from this landing page.

Optionally, you could also give us links for blogs, webinars, demo videos, and/or white papers. We will also link to those from our partner page.

### **Logo-Large | Required**

Provide a URL to your logo for our /security-hub/partners/ page. Logo must be 600x300 pixels, tightly cropped with no padding, have a clear background and be in PNG format.

### **Logo-Small | Required**

Provide a URL to your logo for our console. Logo must be 175x40 pixels, tightly cropped with no padding, have a clear background and be in PNG format. See Appendix B for detailed guidelines.

### **findingTypes | Required**

Please provide a table that documents the ASFF-formatted finding types that you use and how they align to your native finding types. We recommend that you include this in your product documentation as well. See [AWS Finding Format finding type taxonomy appendix for details](#).

### **Hotline | Required**

Please provide an email address and phone number/pager number for a technical point of contact that we can contact any technical issues (e.g., an integration is no longer working). Please also provide a 24/7 point of contact of high severity technical issues.

### **Heartbeat Finding | Required**

Can you send Security Hub a “heartbeat” finding every five minutes that indicates that your integration with Security Hub is functional? If so, please do so, using the Finding Type: Heartbeat.

## **Security Hub Console Information**

Instructions: Please submit JSON text back to the Security Hub team with the information below. This text can be in red pasted directly into this Word document. We will use this information to create your productArn, populate our Provider page in our console, and populate our Insight library with your proposed default Insights.

For guidance on the console card, please refer to **Appendix B – Integration Logo Guidelines**

## **Company Information**

### **Template example:**

```
{
  "id": "acme",
  "name": "ACME",
  "description": "ACME is a network security company that...",
}
```

### **id : string | Required**

The company's unique identifier. These must be unique across companies. This is likely the same or similar as name. [a-z][-a-z0-9]{3,22}[a-z0-9]

**name : string | Required**

The name of the provider's company to be displayed in the Security Hub console. **16 characters max.**

**description : string | Required**

The description of the provider's company to be displayed in the Security Hub console. **200 characters max.**

## Product Information

**Template example:**

```
{
  "IntegrationType": "SEND_FINDINGS_TO_SECURITY_HUB",
  "id": "acme-network-defender",
  "regionsNotSupported": "us-gov-east-1",
  "commercialAccountNumber": "123456789012",
  "govcloudAccountNumber": "012345678901",
  "chinaAccountNumber": "012345678999",
  "name": "ACME Network Defender",
  "description": "ACME Network Defender is a managed threat detection
service that...",
  "importType": "BATCH_IMPORT_FINDINGS_FROM_CUSTOMER_ACCOUNT",
  "category": "Intrusion Detection Systems (IDS)",
  "marketplaceUrl": "marketplace_url",
  "configurationUrl": "activation_url"
}
```

**IntegrationType : string | Required**

Denotes if your product will send, receive, or both send and receive findings to / from Security Hub. If you are a CP, leave blank.

Valid Values: SEND\_FINDINGS\_TO\_SECURITY\_HUB |  
RECEIVE\_FINDINGS\_FROM\_SECURITY\_HUB

**id : string | Required**

The product's unique identifier. These must be unique within a company (but not across companies). This is likely the same or similar as name. [a-z][-a-z0-9]{3,22}[a-z0-9]

**regionsNotSupported : string | Required**

Which of the following regions do you **not** support (i.e., which regions should Security Hub not show you as an option in our partners page in our console)? Please product the region code only (e.g., us-east-1). A list of commercial region codes are [here](#). GovCloud region codes are us-gov-west-1 and us-gov-east-1. China region codes are cn-north-1 (for Beijing) and cn-northwest-1 (for Ningxia).

**commercialAccountNumber : string | Optional**

The primary AWS account number for the product associated with standard commercial regions. If you are submitting findings to Security Hub from your AWS account (as opposed to from

within a customer's account), this account number must be the account number that you are using to submit findings. If you won't be submitting findings from your AWS account to AWS Security Hub, we recommend that this be the primary account that you will be using to test the product integration with Security Hub. Ideally you will use the same account for all of your products across all commercial regions, but let us know if that doesn't work for you. If you are only receiving findings from Security Hub, this can be any account that you own in a commercial region.

**govcloudAccountNumber : string | Optional**

The primary AWS account number for the product associated with GovCloud regions (if your product is available in GovCloud). If you are submitting findings to Security Hub from your AWS account (as opposed to from within a customer's account), this account number must be the account number that you are using to submit findings. If you won't be submitting findings from your AWS account to AWS Security Hub, we recommend that this be the primary account that you will be using to test the product integration with Security Hub. Ideally you will use the same account for all of your products across all GovCloud regions, but let us know if that doesn't work for you. If you are only receiving findings from Security Hub, this can be any account that you own in a GovCloud region.

**chinaAccountNumber : string | Optional**

The primary AWS account number for the product associated with China regions (if your product is available in the China regions). If you are submitting findings to Security Hub from your AWS account (as opposed to from within a customer's account), this account number must be the account number that you are using to submit findings. If you won't be submitting findings from your AWS account to AWS Security Hub, we recommend that this be the primary account that you will be using to test the product integration with Security Hub. Ideally you will use the same account for all of your products across all China regions, but let us know if that doesn't work for you. If you are only receiving findings from Security Hub, this can be any account that you own in a China region.

**name : string | Required**

The name of the provider's product to be displayed in the Security Hub console. **24 characters max.**

**description : string | Required**

The description of the provider's product to be displayed in the Security Hub console. **200 characters max.**

**importType : string | Required**

We have two types of resource policies for partners:

BATCH\_IMPORT\_FINDINGS\_FROM\_PRODUCT\_ACCOUNT and  
BATCH\_IMPORT\_FINDINGS\_FROM\_CUSTOMER\_ACCOUNT.

During the partner onboarding process, you can request to receive either, one or neither. With the PRODUCT\_ACCOUNT one, you can only send findings to SecHub from the account listed in your product ARN. With the CUSTOMER\_ACCOUNT one, you can only send findings from the customer account that subscribed to you.

Valid values:

BATCH\_IMPORT\_FINDINGS\_FROM\_PRODUCT\_ACCOUNT  
BATCH\_IMPORT\_FINDINGS\_FROM\_CUSTOMER\_ACCOUNT  
NEITHER

**category : array | Required**

These are the category(s) that define your product, and your selections will appear in the Security Hub console. Choose up to **three** selections. Custom selections are not allowed, but please let us know if you think your category is missing.

API Firewall	Interactive Application Security Testing (IAST)
Asset Management	Instant Messaging
AV Scanning and Sandboxing	IoT Security
Backup and Disaster Recovery	IT Security Training
Breach and Attack Simulation	IT Ticketing and Incident Management
Bug Bounty Platform	Managed Security Service Provider (MSSP)
Certificate Management	Micro-Segmentation
Cloud Access Security Broker	Multi-Cloud Management
Cloud Security Posture Management	Multi-Factor Authentication
Configuration and Patch Management	Network Access Control (NAC)
Configuration Management Database (CMDB)	Network Forensics
Consulting Partner	Network Intrusion Detection Systems (IDS)
Container Security	Network Intrusion Prevention Systems (IPS)
Cyber Range	Phishing Simulation and Training
Data Access Management	Privacy Operations
Data Classification	Privileged Access Management
Data Loss Prevention	Rogue Device Detection
Data Masking and Tokenization	Runtime Application Self-Protection (RASP)
Database Activity Monitoring	Secure Web Gateway
DDoS Protection	Security Data Lake
Deception	Security Information and Event Management (SIEM)
Device Control	Security Orchestration, Automation, and Response (SOAR)
Dynamic Application Security Testing	Serverless Security
Data Encryption	Single Sign On (SSO)
Email Gateway	Software Composition Analysis
Encrypted Search	Static Application Security Testing (SAST)
Endpoint Detection and Response (EDR)	Third-Party Risk Assessment
Endpoint Forensics	Threat Intelligence Platform

Network Firewall	Threat Modeling
Forensics Toolkit	User and Entity Behavior Analytics (UEBA)
Fraud Detection	Virtual Private Network
Governance, Risk, and Compliance (GRC)	Vulnerability Assessment and Management
Host-based Intrusion Detection (HIDs)	Web Application Firewall (WAF)
Human Resources Information System	Zero Trust Network Access

**marketplaceUrl : string | Optional**

The URL to the provider's product AWS Marketplace destination to be displayed in the Security Hub console. This must be an AWS Marketplace URL. If you do not have a Marketplace listing, please leave blank.

**configurationUrl : string | Required**

This is URL to the your product documentation about the integration with Security Hub is hosted on your website or a webpage managed by you (e.g., your GitHub page). Your documentation should include configuration instructions, links to CloudFormation templates (if necessary), information about your use case for the integration, latency, ASFF mapping, types of findings included, and architecture.

## Appendix A – Product Readiness Checklist

This is the checklist that the AWS Security Hub and/or AWS Partner team uses to validate that the integration is ready for a GA launch.

Question	Context
<b>ASFF Mapping Questionnaire</b>	
Does all of the partner's finding data get mapped into ASFF?	All findings from a provider should be mapped in some way to the ASFF. Curated fields such as modeled resource types, Network, Malware or Threat Intelligence should be used. Anything else should be modeled into Resource.Details.Other or Product Fields as appropriate
Does the partner utilize Resource.Details fields (EC2 Instance, Container, Other, Etc)?	Findings should use the provided fields for curated resources (EC2 Instance, S3 Bucket, Security Group, etc) when possible. Other information related to resources should be mapped to Resource.Details.Other only when there is not a direct match.
Does the partner utilize the Resource.Details.Other field to define extra resource details not modeled in the ASFF?	
Does the partner map values to UserDefinedFields?	User Defined Fields should not be used, please consider using another curated field, Resource.Details.Other or Product Fields in that order
Does the partner map information into ProductFields that could be mapped into other ASFF fields?	The only information that should be mapped into Product Fields are product-specific information such as a versioning information, product-specific severity findings, or other information that cannot be mapped into a curated field or Resources.Details.Other



<p>Does the partner import their own timestamps for the "FirstObservedAt" field?</p>	<p>The "FirstObservedAt" timestamp is meant to retain the time from when a finding was observed in the Product and should map that time over when at all possible</p>
<p>Does the partner provide unique values generated for each finding ID except for findings that they want to be updated?</p>	<p>All findings in Security Hub are indexed on the finding "ID". This value should always be unique to ensure findings are not updated accidentally. This finding "ID" state should also be maintained by a partner for the purpose of updating the findings</p>
<p>Does the partner provide a value that maps findings to a Generator ID?</p>	<p>Generator ID should not have the same value as the finding "ID". Generator ID should be able to logically tie together findings by what generated them. This can be a sub-component within a Product (Product A - Vulnerability vs Product A - EDR) or similar</p>
<p>Does the partner use the required Finding Types namespaces in a way that is relevant to their product?</p>	<p>The Finding Type Taxonomy should closely map to what findings are generated by the Product. You can however use customer Categories or Classifiers (2nd and 3rd level namespaces). The first level namespaces outlined in the AWS Security Finding Format are required.</p>
<p>Does the partner use the recommended finding Type categories or classifiers in their finding Types?</p>	
<p>Does the partner capture network flow information in the Network fields, if they have network data?</p>	<p>If NetFlow information is captured by the partner product, it should be mapped to the Network field.</p>

Does the partner capture process (PID) information in the Process fields, if they have process data?	If process information is captured by the partner product, it should be mapped to the Process field.
Does the partner capture malware information in the Malware fields, if they have malware data?	If malware information is captured by the partner product, it should be mapped to the Malware field.
Does the partner capture threat intelligence information in the Threat Intelligence fields, if they have threat intel data?	If threat intel information is captured by the partner Product, it should be mapped to the Threat Intelligence field.
Does the partner provided a confidence rating for findings and is a rationale provided?	Whenever this field is utilized, partners should provide rationalization in their documentation and Manifest.
Does the partner use canonical ID or ARNs for the Resource ID in the finding?	When identifying AWS resources, the best practice is to use the ARN. If an ARN is not available, use the canonical resource ID.
<b>Integration Questionnaire</b>	
Does the partner provide an Infrastructure-as-Code (IAC) Template to deploy the integration with Security Hub? (Terraform, CFN, CDK, etc)	For Integrations that will send findings from the Customer Account or consume findings via CloudWatch Events, there MUST be some form of IAC template to stand up this integration. CloudFormation is preferred, but CDK or Terraform can also be used.
Does the partner Product have a "one-click" integration setup with Security Hub from their console?	Some partner product's utilize a toggle or similar mechanism in their product to activate the integration. This may entail automatically provisioning resources and permissions, or otherwise. For partners sending findings from a Product Account, this is the preferred method.
Is the partner only sending findings of value?	Partners should generally only send findings that have security value to Security Hub's customers. Security Hub is not a general log management tool and so partners should avoid sending every possible log to Security Hub.
Did the partner provide an estimate on how many findings they will send per day per customer and at what frequency (average and burst)?	Numbers of unique findings are used to calculate load on Security Hub. A unique finding is defined as a finding with a different ASFF mapping than another. For instance, if you provide findings that only populated Threat Intelligence and another that only populated Resources.Details.Ec2Instance that would be 2 unique findings
Does the partner have a graceful way of handling 4xx and 5xx errors such that they are not throttled and all findings can be sent at a later time?	There is currently a 30-50 TPS burst rate on the BatchImportFindings API. If 4xx or 5xx errors are returned, partners must retain the state of those failed findings to be retried in totality later. This can be done via a Dead Letter Queue or using other AWS messaging services such as SNS or SQS

Does the partner maintain the state of their findings so that they know to archive findings that are no longer present?	For partners that will be updating findings via overwriting the original finding "ID" there must be a mechanism to retain state so the correct information is updated for the correct finding. The UpdateFinding API should not be used by finding providers and should only be used by customers or taking action partners.
Does the partner handle retries in a way that won't compromise previously sent successful findings?	partners should have a mechanism to retain the original finding IDs in the case of errors so that successful findings are not duplicated or overwritten in error
Does the partner update findings by calling the BatchImportFindings API with the existing findings' finding "ID"?	Findings must be updated by partners by overwriting the existing finding by submitting the same ID. The UpdateFindings API should only be used by customers.
Does the partner update findings using the UpdateFindings API?	Taking action partners may update specific fields using the UpdateFindings API
Does the partner provide information on how much latency there is between findings being created and being sent to Security Hub from their Product?	Partners should minimize latency to ensure that customers see findings as soon as possible in Security Hub. This is required in the Manifest
If the partner's architecture is to send findings to Security Hub from a customer account, have they demonstrated this successfully?	During testing, findings must be successfully sent from a partner's account other than the account provided for the Product ARN. Sending from the Product ARN owner account can bypass certain error exceptions from the APIs
If the partner's architecture is to send findings to Security Hub from their own account, have they demonstrated this successfully?	
Does the partner provide a heartbeat finding to Security Hub?	partners should send a heartbeat finding using the Finding Type: Heartbeat every 5 minutes to show their integration is working correctly. This is important for partners sending findings from a Product Account.
Did the partner integrate with the Security Hub PM account during testing?	During pre-Prod validation, finding examples should be sent to the Security Hub Product team's AWS account to demonstrate the findings send and map correctly
<b>Documentation Questionnaire</b>	
Does the partner host their documentation on a dedicated website?	Documentation should be hosted on the partner's website either in the form of static webpage, Wiki, ReadTheDocs or some other dedicated format. Hosting documentation on GitHub does not satisfy the "dedicated website" requirement.

Does the partner provide instructions on how to set up the Security Hub integration in their documentation?	This could be via either IAC template or console-based "one-click" integration
Does the partner provide a description of their use case in their documentation?	Is the use case provided in the Manifest also described in the documentation
Does the partner provide a rationale for the findings they send in their documentation?	Rationale for what types of findings should be provided. For instance, if your Product produces findings for Vulnerabilities, Malware, and Anti-Virus but you only are sending Vuln and Malware findings to Security Hub, rationale should be provided for why.
Does the partner provide a rationale for how they map to ASFF in their documentation?	Rationale for the mapping of a Product's native finding to ASFF should be provided as customers would want to know where to look for specific product information
Does the partner provide guidance on how they updated findings in their documentation, if they are updating findings?	Information about how you retain state, ensure idempotency and overwrite findings with up-to-date information should be provided to customers
Does the partner describe finding latency in their documentation?	Partners should minimize latency to ensure that customers see findings as soon as possible in Security Hub. This is required in the Manifest
Does the partner describe how their severity scoring maps to the ASFF severity scoring?	Mapping information for Product Severity ratings from the Product's native severity ratings should be given. For instance, if you Letter Grade (A,B,C), there should be a rubric given how it maps to the ASFF severity fields.
Does the partner provide rationale for Confidence ratings in their documentation?	If providing Confidence scores, these scores should be ranked as provided. Additional context should be given if you are using statically populated confidence scores or using AI/ML derived mapping
Does the partner note which regions they do/do not support in their documentation?	Regions that are / are not supported should be noted so customers can know which regions to not attempt an integration in
<b>Product Card Information</b>	
Is the provided AWS Account ID valid and 12-digits?	Account ID's are 12-digits, if an account ID less than 12 digits is pushed, then the Product ARN will not be valid
Is the product description =< 200 characters?	The Product Description provided in the JSON within the Manifest should be no longer than 200 characters including spaces
Does the configuration link lead to documentation for the integration?	The configuration link should lead to where you have your documentation hosted. It should not lead to your main website or marketing webpages
Does the purchase link (if provided) lead to the AWS	If you provide a purchase link, it MUST be for an AWS Marketplace entry. We will not accept non-AWS hosted purchased information

Marketplace listing for the product?	
Do the Product Categories correctly describe the product?	In the Manifest up to 3 Product Categories were provided. These should match the JSON, are not custom and no more than 3 should be provided
Is the Company name =< 16 characters??	Does the name in the Product Card JSON match the name in the Manifest?
Is the Product name =< 24 characters??	
<b>Marketing Information</b>	
Is the Security Hub partners page product description within 700 characters to include spaces?	The Security Hub partner Program webpage only accepts up to 700 characters (to include spaces). Excess will be edited down for by the CMS team otherwise
Is the Security Hub partners page logo no larger than 600x300px?	Provide a publicly accessible URL with a company logo in PNG or JPG no larger than 600x300 pixels
Does the "Learn more" hyperlink on the Security Hub partners page lead to the partner's dedicated webpage about the integration?	The "Learn more" link should NOT lead to the partner's main website, nor should it lead to the documentation information. This link should always go to a dedicated webpage with marketing information about the integration.
Does the partner provide a demo / instructional video for using their Integration?	A demo or integration walkthrough video is an optional, but recommended, addition to the partnership & integration
Is an APN Blog Post being released with the partner and their PDM/PDR?	APN Blog Posts should be coordinated ahead of time with the partner Development Manager / partner Development Rep. These are separate from any Blog post a partner creates themselves. Allow for 4 - 6 weeks lead time, this effort should be started after testing with the Private Product ARN is complete
Is a partner-led press release being released?	partners can work with their partner Development Manager / partner Development Rep to get a quote from the External Security Services' VP, Dan Plastina for purpose of using it in their PR release
Is a partner-led blog post being released?	partners can create their own Blog posts showcasing the integration outside of the APN Blog Post
Is a partner-led webinar being released?	partners can create their own Webinars showcasing the integration. If assistance from the Security Hub team is required, work with the PMs after testing with the Private Product ARN is complete
Did the partner request social media support from AWS?	partners can work with the AWS Security Marketing Lead post-release to utilize AWS official social media channels to share details about partner-led webinars



# Appendix B – Logo Guidelines for Security Hub Console

## Format

PNG file format

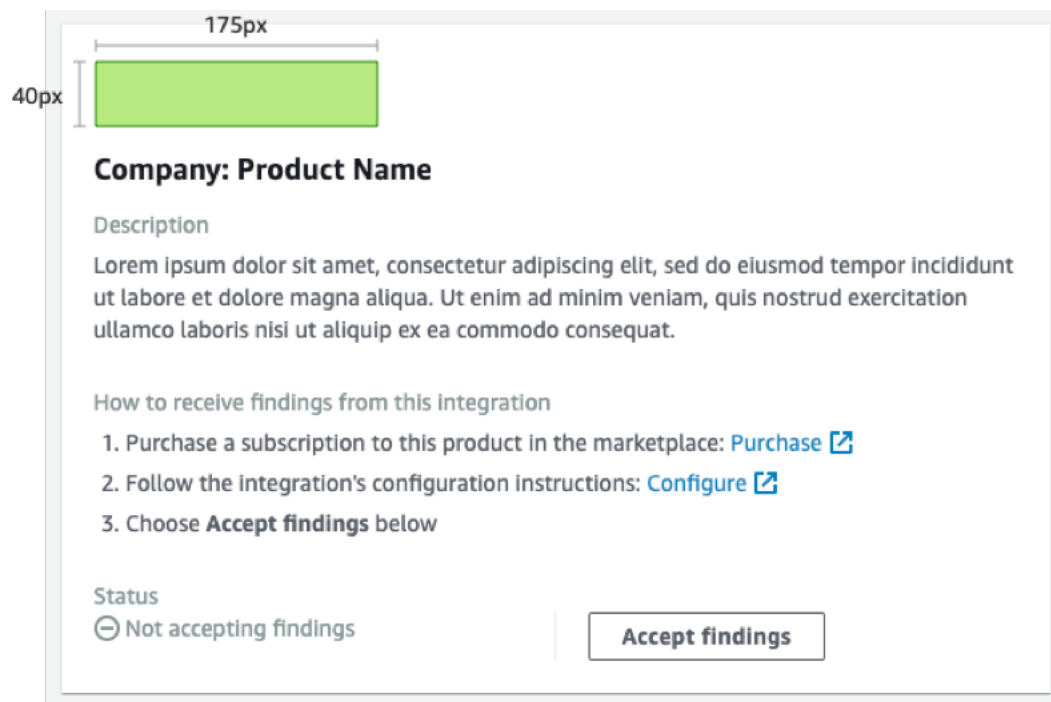
---

## Background Color

1. Preferably transparent background
  2. If not transparent, solid white background
- 

## Sizing


1. Ideal size is 175px × 40px
2. Minimum height is 40px



1. If you provide a logo that does not match the ideal dimensions, that's ok, but we will reduce the size to have a maximum height of 40px and a maximum width of 175px. Notice that this will affect how it looks on the integration cards. Rectangular logos work best.

✔ Original size: 175px × 40px



 **EXAMPLE**

**Company: Product Name**

Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

How to receive findings from this integration


1. Purchase a subscription to this product in the marketplace: [Purchase](#)
2. Follow the integration's configuration instructions: [Configure](#)
3. Choose **Accept findings** below

Status

Not accepting findings

✘ Original size: 133px × 75px (reduced to 70px × 40px)



 **EXAMPLE**

**Company: Product Name**

Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

How to receive findings from this integration


1. Purchase a subscription to this product in the marketplace: [Purchase](#)
2. Follow the integration's configuration instructions: [Configure](#)
3. Choose **Accept findings** below

Status

Not accepting findings

✘ Original size: 275px × 40px (reduced to 175px × 29px)



 **WIDER EXAMPLE**

**Company: Product Name**

Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

How to receive findings from this integration

1. Purchase a subscription to this product in the marketplace: [Purchase](#)
2. Follow the integration's configuration instructions: [Configure](#)
3. Choose **Accept findings** below

Status

Not accepting findings


## Cropping

1. Crop the logo image as close as possible (do not provide extra padding)



✔ Cropped closely



 **EXAMPLE**

**Company: Product Name**

Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

How to receive findings from this integration


1. Purchase a subscription to this product in the marketplace: [Purchase](#)
2. Follow the integration's configuration instructions: [Configure](#)
3. Choose **Accept findings** below

Status

Not accepting findings

✘ Extra padding makes logo look smaller and misaligned



 **EXAMPLE**

**Company: Product Name**

Description

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

How to receive findings from this integration

1. Purchase a subscription to this product in the marketplace: [Purchase](#)
2. Follow the integration's configuration instructions: [Configure](#)
3. Choose **Accept findings** below

Status

Not accepting findings

# Appendix C – Technical Design Principles

## Design principles for the BatchImportFindings API

- Send the largest batch you can - we accept up to 100 Findings or 240kb per batch, whichever comes first
- Our Throttle Rate Limit is 10TPS, with a burst of 30TPS.
- You must implement a mechanism to retain state of findings in the event of being throttled or network issues as well as to submit finding updates as a finding moves in and out of compliance
- Refer to our public docs for max lengths of strings or other limitations: <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-findings-format.html>

## Design principles for mapping into the ASFF

- SchemaVersion is always 2018-10-08
- Finding Id is what we index off of, and it must be unique to ensure other findings are not overwritten
  - In the case of updating findings, you should resubmit the finding with the same Id
- We will assign you a ProductArn
- GeneratorId can be the same as your finding ID, or can refer back to a discrete unit of logic (e.g. GuardDuty Detector ID, Config Recorder ID, IAM Access Analyzer ID)
- Finding Types should match against the [Types Taxonomy of the ASFF](#), in certain occasions it may make sense to submit a custom Classifier (the 3rd namespace), use your discretion here
- CreatedAt and UpdatedAt must be submitted every time BIF is called per finding
  - Must match to ISO8601 format, in Python 3.8:  
`datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()`
- FirstObservedAt and LastObservedAt must match against when the finding was found on your side, if you do not record this you do not need to submit these timestamps
  - Must match to ISO8601 format, in Python 3.8:  
`datetime.datetime.utcnow().replace(tzinfo=datetime.timezone.utc).isoformat()`
- For Severity scores refer to our ASFF documentation for which values map into which qualitative labels in our console (Informational, Low, Medium, High and Critical)
  - Findings that are compliant should always have a “0” for Severity values, examples of this are Security Hub CIS findings that are passing or Firewall Manager findings that have been remediated

- Customers often sort findings by their severity to give their SecOps teams a “to-do” list, be conservative when setting High & Critical severity on your findings.
  - Your mapping rationale **must** be in your documentation regarding the integration
- Confidence scores (0-99) should only be included if your service has a similar functionality, or if you stand 100% by your finding
  - Currently we do not expose this in our UI, it is only within the finding
- Criticality scores (0-99) are intended to express the importance of the resource associated with the finding.
  - Currently we do not expose this in our UI, it is only within the finding
- Your Title should contain some information about the impacted resource, but expansive detail should be added into Description.
  - Titles can only be 256 chars long (including spaces) and Descriptions can only be 1024 chars long (including spaces). You can consider adding truncation to Descriptions
  - example: **Title:** Instance i-12345678901 is vulnerable to CVE-2019-1234 **Description:** Instance i-12345678901 is vulnerable to CVE-2019-1234, this vulnerability affects version 1.0.1 of widget-1 and earlier and can lead to buffer overflow when someone sends a ping.
- Remediation has two elements which are combined in the Console. Remediation.Recommendation.Text appears in its own section of the Findings UI, and it will be hyperlinked by the value you place into Remediation.Recommendation.Url
  - Currently, our compliance standards, IAM Access Analyzer and Firewall Manager only put text suggesting the customer select the hyperlink which links to documentation on how to remediate the finding
- SourceUrl should only be used if you can provide a deep-linked URL to your console for that specific finding. If not, leave it out of the mapping
  - Currently, we do not support hyperlinking from this field, but it will be exposed in the UI
- ProductFields should **only** be used in the event that you cannot use another curated field for Resources or a descriptive object like ThreatIntelIndicators, Network, Malware, etc.
  - You must provide strict rationale for this decision
- **Never use UserDefinedFields. These are reserved for usage by customers.**
- If you have a use case, please use Malware, Network, Process and/or ThreatIntelIndicators. Each of these objects / lists will be exposed in the UI. These objects / lists should be used in context of the finding that you are sending. For example,

if you notice Malware that is connecting outbound to a known C2 Node, you would make the finding about Resource.AwsEc2Instance and fill out the relevant Malware, Network and ThreatIntelIndicator objects for that specific EC2 instance.

- Malware-Specific Principles

- This is a list that will accept up to 5 arrays of malware information. Make the malware entries relevant to the resource and the finding
- Name and Path will accept strings 64 and 512 characters each, respectively. Name should ideally be from a vetted threat intel or researcher source. Path should always be a Linux / Windows system filepath, though there are some exceptions
  - If you are scanning objects in a S3 Bucket or EFS Share against Yara rules (AirBnB does with this [BinaryAlert](#) and there is also [awss3VirusScan](#)) then your path would be the S3:// or HTTPS object path
  - If you are scanning files in a Git repo then the path should be the Git URL / Clone path
- State has enum backed strings of OBSERVED | REMOVAL\_FAILED | REMOVED. Discretion should be taken here to ensure you contextualize what happened with the malware in the Title / Description of your finding
  - For instance, Malware.State = REMOVED then your finding title / description should reflect that your product was able to remove the malware located on path X
  - Other example, Malware.State = OBSERVED then your finding title / description should reflect that your product encountered this malware located on path X
- Type is also enum-backed, if there is a need for an additional Type enum please let us know ADWARE | BLENDED\_THREAT | BOTNET\_AGENT | COIN\_MINER | EXPLOIT\_KIT | KEYLOGGER | MACRO | POTENTIALLY\_UNWANTED | SPYWARE | RANSOMWARE | REMOTE\_ACCESS | ROOTKIT | TROJAN | VIRUS | WORM

- Network-Specific Principles

- Network is a single object, you cannot add multiple network-related details
- Destination and Source make sense from a TCP/VPC flow log/WAF log perspective, but can get dicey when you are describing network information relevant to a finding that happens to be about an Attack. Typically Source would be where the attack originated from but it could have other permutations as listed below. Note, for the customer to easily consume this it should be explained in your documentation and described in Title and Description as well

- A DDOS Attack on an EC2 instance would have the Source information be the attacker (though a real DDOS may be using millions of hosts...), Destination be the Public IPv4 of the EC2 Instance and the Direction would be IN (coming INTO AWS)
    - If Malware observed on your EC2 instance was communicating with a known C2 Node you would have the Source information be the IPV4 address of the EC2 instance and the Destination information be the C2 Node (in that scenario you should also be providing Malware and ThreatIntelIndicators information) and the Direction would be OUT (leaving AWS)
  - Protocol should always map to a IANA registered name unless there is a specific protocol that can be described. You should always use this and provide the Port information
    - Note Protocol is given on its own decoupled from Source / Destination, use it only when it makes sense to
  - Direction should always be taken in relation to AWS' network boundaries. Coming IN means it is entering AWS (VPC, service) and coming OUT means egressing AWS' network boundaries
- Process-Specific Principles
  - Process is a single object, you cannot add multiple process-related details. Given the (likely) reason if you're collecting process information (via RASP/IDS/IPS/EDR/etc) it makes sense to create a single finding per process you encounter anyway
  - There are two time-stamps (LaunchedAt and TerminatedAt) if you cannot reliably retrieve this information and if it is not accurate to the millisecond you should not provide it at all, if a customer relies on time-stamps for forensics investigation the wrong time-stamp is highly egregious
  - Process.Pid and or Process.ParentPid should match the Linux PID or Windows Event ID. To differentiate, information should be provided either via EC2 AMI (customers could probably tell the difference between Windows/Linux). If it is a container that may be harder to do.
  - Process.Path is the filesystem path to the process executable, this accepts up to 512 characters
  - Process.Name should match what the executable's name, it accepts up to 64 characters
- ThreatIntelIndicators Specific Principles
  - Threat intel accepts an array of up to 5 threat intel objects
  - ThreatIntelIndicators.Type is enum-backed, this should be in context of the specific threat DOMAIN | EMAIL\_ADDRESS | HASH\_MD5 | HASH\_SHA1 | HASH\_SHA256 | HASH\_SHA512 | IPV4\_ADDRESS | IPV6\_ADDRESS | MUTEX | PROCESS | URL

- If you found a Process that you know to be associated with Cobalt Strike because you learned that from FireEye’s blog you would set the type to PROCESS. You should ideally create a Process object as well denoting that
  - If your Web Mail Filter found someone sending a well known hashed package from a known malicious domain ([peter.parker@microsoft.net](mailto:peter.parker@microsoft.net)) you would probably do **two** ThreatIntelIndicator objects, one for the DOMAIN and one for the HASH\_SHA1
  - If you found malware with a Yara rule (Loki, Fenrir, Awss3VirusScan, BinaryAlert) that would be **two** as well, one for the Malware and the other for the HASH\_SHA1
- For Resources use our curated resources and detail fields whenever possible, we are constantly adding new resources to the ASFF, please contact [securityhub-partners@amazon.com](mailto:securityhub-partners@amazon.com) to get a monthly changelog
  - If you cannot fit the information in a curated resource’s details, map the “overflow” to Resource.Details.Other
  - If you are trying to map findings for a non-modeled resource, use Resource.Type of “Other” and then use Resource.Details.Other for the detailed information
    - This can be used to express non-AWS findings as well
- Compliance Status should only be used if your findings are compliance oriented in nature
  - Security Hub uses Compliance for our compliance standards findings, unsurprisingly
  - Firewall Manager uses Compliance for their findings as they are compliance-related in nature
- Do not use VerificationState or WorkflowState. These are for usage by customers or ticketing/SOAR systems, not finding providers. Finding providers can update RecordState.
- You should use RelatedFindings **only** if you can keep track of findings related to the same resource or finding Type
  - You will need to reference the ID of a finding that is already in Security Hub, hence the need to maintain state of what findings you will send
- Note should not be used, that is for customers to use who utilize the UpdateFindings API